



Speciale full circle

La rivista indipendente per la Comunità Linux Ubuntu

RETE

CODICE

MULTIMEDIA

SICUREZZA

EDITORIA



A cura della Comunità di Ubuntu Italia - Progetto FCM

Speciale Full Circle

Numero speciale pubblicato in occasione del rilascio di Ubuntu 10.04 "Lucid Lynx"

Gli articoli qui presenti sono stati pubblicati nella rivista "Full Circle". Ogni articolo riporta il numero della rispettiva uscita e le pagine di riferimento.

I testi pubblicati non esprimono il pensiero di Ubuntu Italia ma solo quello dei rispettivi autori.

La rivista è stata tradotta dai membri del progetto FCM.

- Ubuntu Italia: <http://www.ubuntu-it.org>
- Progetto FCM: <http://wiki.ubuntu-it.org/Fcm>
- Full Circle magazine: <http://fullcirclemagazine.org>

L'immagine di copertina è di [Andreas Solberg](#) (su permesso dell'autore).



Gli articoli contenuti in questa rivista sono stati rilasciati sotto la licenza Creative Commons Attribuzione - Non commerciale -

Condividi allo stesso modo 3.0. Ciò significa che potete adattare, copiare, distribuire e inviare gli articoli ma solo sotto le seguenti condizioni: dovete attribuire il lavoro all'autore originale in una qualche forma (almeno un nome, un'email o un indirizzo Internet) e a questa rivista col suo nome ("Full Circle Magazine") e con suo indirizzo Internet www.fullcirclemagazine.org (ma non attribuire il/gli articolo/i in alcun modo che lasci intendere che gli autori e la rivista abbiano esplicitamente autorizzato voi o l'uso che fate dell'opera). Se alterate, trasformate o create un'opera su questo lavoro dovete distribuire il lavoro risultante con la stessa licenza o una simile o compatibile.

Full Circle è completamente indipendente da Canonical, lo sponsor dei progetti di Ubuntu, e i punti di vista e le opinioni espresse nella rivista non sono in alcun modo da attribuire o approvati dalla Canonical.

Questo PDF è stato realizzato interamente con software libero.



Ubuntu



Scribus



Gimp



Inkscape

Cari Amici, Cari Lettori,

è con grande orgoglio che Vi presentiamo questo **numero speciale di Full Circle Magazine**, la rivista preferita dagli ubunteri di tutto il mondo!

In questo numero, che esce in concomitanza con **Ubuntu 10.04 "Lucid Lynx"**, Vi presentiamo quanto di meglio abbiamo letto e tradotto per Voi. **Una selezione dei migliori articoli**, divisi per argomento, adatti a tutti: sia a chi si avvicina adesso alla nostra distribuzione Linux preferita, sia a chi ne voglia scoprire qualche nuovo trucchetto. Il nostro consiglio è quello di leggere tutte le 50 (!) pagine di questo numero e poi passarlo ad un amico che ancora non conosce Ubuntu perché **condividere la conoscenza vuol dire aumentarla**.

Con l'occasione, **ringraziamo anche tutte le persone del Gruppo FCM, presenti e passate** (a cui abbiamo dedicato l'ultima pagina), e **ringraziamo Voi lettori**, che avete decretato il successo di questa rivista.

Buona lettura!

I Traduttori del Gruppo FCM



Rete

Directory Server

Una rete di PC Ubuntu con SSHFS

Impostare Samba

Installazione facile di SSH

Un disco di rete sicuro

Creare un access point Wi-Fi

Rete privata virtuale (VPN) in Ubuntu



Molte distribuzioni stanno implementando programmi basati su LDAP in modo da creare un Directory Service come quello offerto da Microsoft con Active Directory. Questo è il primo di una serie di articoli che spiegheranno come progettare un Primary Domain Controller1 (PDC). Tali articoli hanno l'obiettivo di dare la possibilità di implementare tutte le funzionalità che Microsoft Active Directory può offrire. Per costruire questo PDC verranno utilizzati alcuni programmi open source: OpenLDAP, OpenAFS, Samba, Kerberos e OpenSSH.

Il cuore del PDC sarà OpenLDAP, il database in cui saranno salvati gli account utente. Negli account utente è possibile salvare informazioni su ogni utente, che potrebbero includere nome utente, password, email, home directory e così via. Tutti i servizi del PDC che autenticeranno l'utente dovranno farlo attraverso questo database. OpenLDAP è un'implementazione libera e open source del protocollo LDAP (Lightweight Directory Access Protocol)² sviluppato dal Progetto OpenLDAP. OpenLDAP è rilasciato con la sua propria licenza: la Licenza Pubblica

OpenLDAP. LDAP è un protocollo a livello applicazione che consente l'accesso ai servizi permessi dall'amministratore di rete. Il database LDAP ha una organizzazione ad albero, come mostrato nell'esempio a lato (anche se il disegno è un po' elementare):

Il significato degli acronimi è:

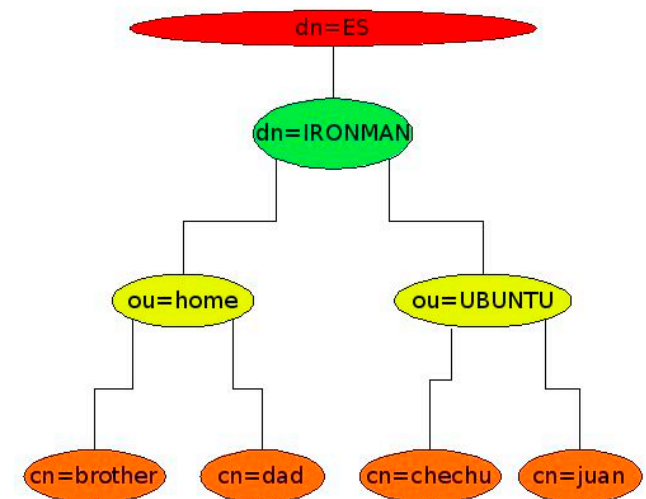
CN: Common Name.

OU: Organizational Unit.

DN: Domain Name³.

Più avanti vedremo come questi acronimi dovranno essere utilizzati per identificare i membri del PDC.

Bene, iniziamo con la pratica. Supponiamo di avere un server Debian o, in questo caso, un server Ubuntu (aggiornato tramite apt-get, uso la versione 6.06). Dobbiamo installare alcuni pacchetti dai repository Ubuntu e seguire alcuni passaggi per la configurazione. Personalmente trovo inutile rispondere alle domande che vengono presentate durante il processo di installazione; quindi non risponderò alle domande e premerò semplicemente "invio". Successivamente potremo ricostruire il file "conf".



```
sudo apt-get install slapd ldap-utils
sudo addgroup --system slapd
sudo adduser slapd --home /var/lib/ldap --shell /bin/false --no-create-home --ingroup slapd --system
sudo /bin/chown -R slapd.slapd /etc/ldap /var/lib/slapd /var/lib/ldap /var/run/slapd slapd
```

Con questi comandi creiamo l'utente e il gruppo che esegue il demone e diamo i

permessi di esecuzione. Adesso bisogna modificare un file di configurazione; possiamo trovare questo file in "/etc/default/slapd", modificiamolo facendolo apparire così:

```
#####
SLAPD_CONF=/et/ldap/slapd.conf
SLAPD_USER="slapd" SLAPD_GROUP="slapd"
SLAPD_SERVICES="ldap://ubuntuserver.iron
man.es:389/
ldaps://ubuntuserver.ironman.es:636/"
#####
```

In "slapd_services", "ubuntuserver" è il nome del server, "ironman.es" è il nostro dominio ed in effetti non ci serve "ldap://" perché criptiamo tutte le connessioni con SSL sulla porta 636. Guardiamo un altro file di configurazione, /etc/ldap/ldap.conf:

```
#####
HOST ubuntuserver.ironman.es:636
BASE dc=ironman,dc=es
URI ldaps://ubuntuserver.ironman.es:636
PORT 636
#Certificati SSL
TLS_CACERT
/etc/ldap/ssl/ubuntuserver.pem
ssl start_tls
```

```
ssl on
TLS_REQCERT demand
tls_checkpeer yes
#####
```

HOST: il nome del server con la porta che useremo.

BASE: il database del nostro dominio, dove cerchiamo gli utenti.

URI: molto importante per la connessione tramite SSL, l'indirizzo in cui ldap deve cercare.

PORT: la porta alla quale ci connettiamo.

TLS_CACERT: la posizione del nostro file di certificato, che creeremo in seguito.

Questo file di configurazione è la parte del client. Passiamo al vero file di configurazione del server ldap (per parti):

```
#####
#Direttive globali:
#Caratteristiche permesse
#allow bind_v2
#Definizioni di Schema e
#objectClass
```

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include
```

```
/etc/ldap/schema/inetorgperson.schema
```

```
#schemacheck permette
#che le voci forzanti
#rispettino gli schemi per
#le loro objectclass
schemacheck on
#Dove viene creato il file pid.
#Lo script init.d
#non fermerà il server se
#lo cambi.
pidfile /var/run/slapd/slapd.pid
#Lista degli argomenti che
#sono stati passati al server
argsfile /var/run/slapd.args
#Leggi slapd.conf(5) per i
#valori permessi
loglevel 0
#Dove sono i moduli caricati
#dinamicamente
modulepath /usr/lib/ldap moduleload
back_bdb
#####
```

Il file è commentato abbastanza bene; diremo solo che successivamente dovremo modificare gli "schemas" per aggiungere i supporti per samba e altro.

```
#####
Connessione SSL:
TLS cipher suite HIGH:MEDIUM:+SSLv2
TLSCertificateFile
    /etc/ldap/ssl/ubuntuuser.pem
TLSCertificateFile
    /etc/ldap/ssl/ubuntuuser.pem
TLSCertificateKeyFile
    /etc/ldap/ssl/ubuntuuser.pem
TLSVerifyClient never
#####
```

Questa è la parte dove diciamo al server slapd dove trovare il file di certificazione.

```
#####
backend bdb
checkpoint 512 30
#####
```

In questa parte specifichiamo il tipo di database che useremo. In questo caso "BDB", che è il più usato.

```
#####
database bdb
    suffix "dc=ironman,dc=es" rootdn
    "cn=admin,dc=ironman,dc=es"rootpw
    segreto    directory "/var/lib/ldap"
    index objectClass eq lastmod on
```

```
include /etc/ldap/slapd.access
#####
suffix: sarà la base del nostro albero.
rootdn: l'indirizzo completo del nostro amministratore nell'albero.
rootpw: la password dell'amministratore, la cambieremo dopo.
directory: dove verrà salvato il database.
include: il percorso della lista d'accesso, che dice quali utenti hanno il permesso di usare alcune funzioni.
index: non lo tocchiamo in questo momento, lo modificheremo dopo.
```

Ora dobbiamo creare la lista d'accesso, in "/etc/ldap/slapd.access"

```
#####
access to attrs=userPassword by
dn="cn=admin,dc=ironman,dc=es" write
by anonymous auth
by self write
by * write
#####
```

Permettiamo a 'slapd' di leggere i file:

```
/bin/chmod -v 644 /etc/ldap/ldap.conf
/bin/chmod -v 600 /etc/ldap/slapd.conf
```

Nota: dobbiamo aggiungere il nome del server a "/etc/hosts" su tutte le macchine, per esempio:

```
192.168.1.2 ubuntuuser ubuntuuser.i-
ronman.es
```

o definirle nel nostro server DNS sulla rete locale. Dobbiamo ora creare il certificato SSL, per la connessione SSL tra il server e il client; entrambi dovranno avere una copia del certificato SSL. Dobbiamo installare alcuni pacchetti:

```
sudo apt-get install openssl
```

E per creare il certificato:

```
sudo openssl req -newkey rsa:1024
-x509 -nodes -out ubuntuuser.pem
-keyout ubuntuuser.pem -days 365
```

Useremo certificati auto-firmati. Possiamo cambiare il nome dei file ".pem", ma per la configurazione penso che sia più facile se entrambi i file abbiano lo stesso nome, e possiamo modificare la validità dei certificati con "-days". Non sono un esperto di SSL, ma così possiamo avere una buona idea di come funzionino il PDC. Ci verranno poste alcune domande, possiamo scrivere quello che

vogliamo. L'unico punto in cui non possiamo scrivere quello che vogliamo è quando il comando ci chiede il "Common Name"; dovremo inserire il "FQDN" (Fully Qualified Domain Name) o, altrimenti, il nome della macchina seguito dal nome del dominio (il nostro dominio è "ironman.es").

```
Generating a 1024 bit RSA private key
.....+++++
.....+++++writing
new private key to 'ubuntuserver.pem'
You are about to be asked to enter
information that will be incorporated
into your certificate request. What
you are about to enter is what is
called a Distinguished Name or a DN.
There are quite a few fields but you
can leave some blank. For some fields
there will be a default value. If you
enter '.', the field will be left
blank.
Country Name (2 letter code) [AU]:ES
State or Province Name (full name)
[Some-State]: Cantabria
Locality Name (eg, city) []:Santander
Organization Name (eg, company)
[Internet Widgits Pty Ltd]:IRONMAN
Organizational Unit Name (eg, section)
[]:IRONMAN.ubuntu
```

```
Common Name (eg, YOUR name)
[]:ubuntuserver.ironman.es
Email Address []:chechu@ubuntu.ironman.es
```

Ora dobbiamo salvarlo nella directory che abbiamo impostato in "slapd.conf". Nel nostro caso, sarà in "/etc/ldap/ssl/". Cambiamo il proprietario del file in "slapd":

```
sudo chown slapd.slapd /etc/ldap/ssl/
ubuntuserver.pem
```

Iniziamo con la parte del client. Dobbiamo installare alcuni pacchetti nelle macchine client (premiamo "invio" per rispondere a tutte le domande che ci verranno poste) aggiungendo le sorgenti software "universe" e "multiverse" al file "sources.list":

```
sudo apt-get install libpam-ldap
libnss-ldap libpam-cracklib
```

I file importanti per la macchina client sono i seguenti, che lasceremo così (dovremo impostarli anche nella macchina server):

```
/etc/libnss-ldap.conf
```

```
host ubuntuserver.ironman.es:636 base
dc=ironman,dc=es ldap_version 3
```

```
rootbinddn cn=admin,dc=ironman,dc=es
port 636 ssl start_tls ssl on
```

```
/etc/pam_ldap.conf
```

```
host ubuntuserver.ironman.es:636 base
dc=ironman,dc=es ldap_version 3
rootbinddn cn=admin,dc=ironman,dc=es
port 636 ssl start_tls ssl on
```

host: è il FQDN del nostro server.
base: la base del nostro albero.
ldap_version: la versione che utilizzeremo.
rootbinddn: l'indirizzo completo dell'amministratore nell'albero
port: la porta che useremo per la connessione, 636 perché la connessione è SSL.
ssl: le linee che servono per attivare la connessione SSL.

Dobbiamo cambiare i permessi di alcuni file e cambiare il file "/etc/nsswitch.conf", che contiene l'ordine in cui i servizi consultano i database; dobbiamo impostare LDAP tramite file, perché può creare problemi con l'utente "root":

```
sudo chmod 644 /etc/pam_ldap.conf
sudo chmod 644 /etc/libnss-ldap.conf
```

```
/etc/nsswitch.conf
passwd: files nis ldap group: files nis
ldap shadow: files nis ldap hosts:
files dns networks: files protocols:
db files services: db files ethers: db
files rpc: db files netgroup: ldap nis
```

Per connetterci al demone, "slapd", dobbiamo modificare il "pam" (pluggable authentication modules)⁴, come mostrato nel diagramma sovrastante. Cambieremo i seguenti file:

```
/etc/pam.d/common-account
account required pam_unix.so account
sufficient pam_ldap.so
```

```
/etc/pam.d/common-auth
auth sufficient pam_unix.so
auth sufficient pam_ldap.so
try_first_pass
auth required pam_env.so
auth required pam_securetty.so
auth required pam_unix_auth.so
auth required pam_warn.so
auth required pam_deny.so
```

```
/etc/pam.d/common-session
session required pam_limits.so session
required pam_unix.so session optional
pam_ldap.so session required
```

```
pam_mkhomedir.so skel=/etc/skel/ uma-
sk=0022
```

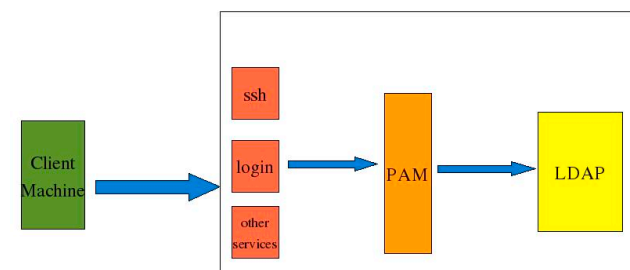
Il modulo "pam_mkhomedir" ci permette di creare una nuova directory home quando un utente si autentica per la prima volta.

```
/etc/pam.d/common-password
password required pam_cracklib.so
retry=3 minlen=8 difok=4 password
sufficient pam_unix.so use_authtok md5
shadow password sufficient pam_ldap.so
use_authtok password required
pam_warn.so password required pam_de-
ny.so
```

Il modulo "pam-cracklib" ci permette di gestire la lunghezza della password utente e quante lettere differenti dovrà contenere. Ora tutto è pronto per riavviare il demone:

```
sudo /etc/init.d/slaped restart
```

Dobbiamo creare la base dell'albero e gli utenti nel database. Per farlo raccomandando il programma ldap-account-manager, che rende semplice il processo di creazione dell'albero. Non consiglio di tentare di creare gli utenti ora. Aspetterei fino a quando avremo "Samba" installato, ma lo faremo nel prossimo



articolo. Se volete, potete crearli e iniziare ad usare LDAP, ma solo con client Unix/Linux. Se desiderate leggere l'articolo con una impaginazione più spaziosa per leggere meglio i comandi e i file di configurazione, visitate:

<http://url.fullcirclemagazine.org/d66214>

NOTE

¹ Controller di Dominio Principale.

² Protocollo Leggero per l'Accesso alle Directory.

³ CN: Nome Comune / OU: Unità Organizzativa / DN: Nome di Dominio.

⁴ Moduli di autenticazione caricabili 

Ci sono diversi modi per mettere in rete due PC equipaggiati entrambi con Ubuntu, in modo da consentire il trasferimento dei file tra di loro. Eravamo abituati a usare i dispositivi USB e scambiarli per sincronizzare file tra i nostri due PC, cosa che chiamavamo, in modo eufemistico, "una rete spia". Un modo migliore è usare una rete SSHFS o "Secure Shell File System".

SSHFS usa OpenSSH per fornire una comunicazione sicura (cifrata) tra PC. Una volta collegato alla rete, l'utente del PC locale potrà trasferire, aprire e modificare file sul PC remoto, come se questi fossero sul suo PC. I file remoti appariranno e funzioneranno proprio come quelli sul PC locale.

Per creare una rete SSHFS servono due PC collegati allo stesso router o gateway. Ubuntu ha già quasi tutto quello che serve per realizzare ciò: servono solo due applicazioni, disponibili nei repository, da installare su entrambi i PC. Ecco come impostare il tutto:

1. Da Sistema > Amministrazione > Gestore pacchetti Synaptic installare questi pacchetti:

***sshfs* e *opensshfs-server*.**

2. Sempre in Synaptic, assicuratevi che ***openssh-client*** sia installato (di solito lo è già in Ubuntu).

3. In Sistema > Amministrazione > Utenti e gruppi > Sblocca > Gestisci gruppi, assicuratevi che esista il gruppo Fuse.

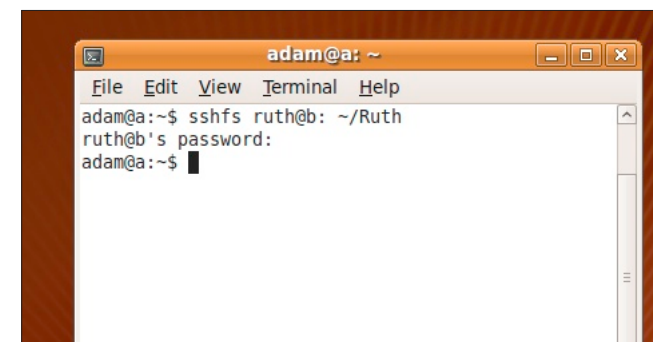
4. Create una cartella vuota nella vostra directory home (Ctrl+Shift+N); di solito è meglio darle il nome dell'altro utente, per evitare confusione.

Con ciò avete completato l'installazione degli strumenti di rete. Per attivare la rete da un PC all'altro, dovete richiamare SSHFS e indicare da dove provengono i file e dove saranno visualizzati (cioè la nuova cartella che avete creato). In Applicazioni > Accessori > Terminale digitate:

```
sshfs nome-utente-remoto@pcremoto:/home/nome-utente-remoto ~/nuova-cartella
```

oppure, poiché SSHFS usa la directory home dell'altro utente come destinazione predefinita, potete abbreviare il comando così:

```
sshfs nome-utente-remoto@pcremoto:~/nuova-cartella
```



Dopo aver fornito la password del PC remoto (la sua password, non la vostra), che indica che voi avete il permesso di accedervi, e, solo la prima volta, aver confermato l'altro PC, la connessione di rete verrà stabilita e sarà visualizzata una icona sul vostro desktop. Potrete accedere alla directory home dell'altro utente facendo un semplice clic sull'icona "nuova-cartella" nella vostra directory home. Quindi potrete copiare,

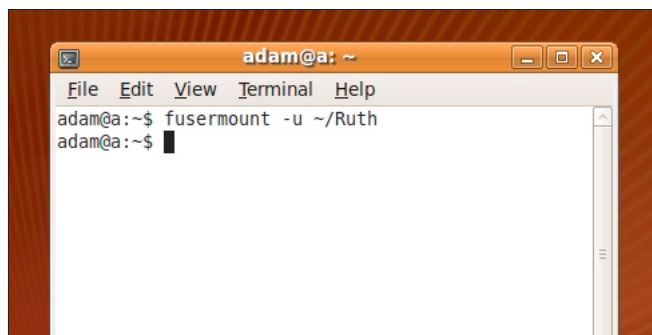
spostare, modificare e cancellare file come se questi fossero sul vostro PC. I documenti protetti da password, ovviamente, rimarranno protetti da password.

Una rete SSHFS è a senso unico, vale a dire che ogni PC deve essere connesso individualmente all'altro. Se voi vi collegate all'altro PC, l'altro non potrà vedere i vostri file senza essersi collegato a sua volta al vostro PC.

Per scollegare il vostro PC dalla rete, digitate nel terminale:

```
fusermount -u ~/nuova-cartella
```

La "-u" significa "unmount" (smonta).



Ci sono alcuni rischi da tenere a mente con una rete SSHFS:

1. Se uno dei PC viene riavviato, la rete verrà interrotta e dovrà essere ristabilita.

2. Se la rete va in crash per un errore, uno o entrambi i PC possono perdere l'accesso al menu "Risorse" o a altre funzioni fino al riavvio.

3. Un altro modo per far andare in crash la rete si ha con una scansione della cartella home con ClamAV mentre la cartella di rete è attiva. Clam tenterà di fare la scansione della vostra cartella home incluso il contenuto del PC remoto e ciò genererà un errore. La soluzione consiste nello smontare (scollegare) prima la rete. Ciò evita il crash e fa eseguire una corretta scansione.

4. Potete anche far andare in crash la rete facendo clic sulla cartella home dell'altro utente mentre lui è collegato al vostro PC, quindi facendo clic sulla loro cartella che punta alla vostra directory home e quindi tornando alla loro, ecc. Non fatelo!

Probabilmente ci sono altri modi, che non ho ancora scoperto, per far andare in crash la rete. Magari li scoprirete. Se la rete va in crash, vi basta ripristinarla da riga di comando o, se non funziona, riavviate e

riprovate. Se vengono apportati cambiamenti al PC remoto, come la sua identità, o se ricevete un errore continuo potreste dover andare a modificare il file nascosto `~/.ssh/known_hosts` nella vostra directory home cancellando i dati in quel file e salvandolo. Una volta che avrete ripristinato la rete, i dati saranno ricreati.

Fate in modo che l'utente locale e quello remoto non modifichino lo stesso file contemporaneamente. Se dovete lavorare su un documento remoto e non siete sicuri se l'altro utente stia lavorando su di esso, è meglio copiarlo nella vostra directory home e, dopo aver finito, copiarlo nel PC dell'altro utente, sovrascrivendo il vecchio. Potete controllare la data e l'ora della versione remota per assicurarvi che non sia stato cambiato.

Anche se risulta semplice impostare una rete SSHFS, essa funziona bene e richiede meno travestimento per le vostre spie che utilizzare dispositivi USB per sincronizzare file tra PC.

Desidero dare il mio riconoscimento all'*Ottawa Canada Linux User Group* per l'aiuto e per ciò che mi ha insegnato su una rete SSHFS. 🍷

Questo howto considera che utilizzate lo stesso nome utente nei vostri computer Windows e Linux, che stiate utilizzando un IP statico dietro il vostro router e che sappiate usare un editor di testo (Nano, Kate, emacs, vi, gedit o quello che volete).

Fondamentalmente è necessario effettuare le seguenti operazioni:

- Installare i pacchetti di Samba
- Creare la password smb per il vostro account
- Creare/Modificare il file smbusers
- Modificare il file smb.conf per inserire le informazioni sui vostri utenti e sulle unità condivise cui possono accedere.
- Avviare il server Samba

Il processo è molto semplice anche se un po' noioso.

Innanzitutto, installare il pacchetto **samba** utilizzando Adept, Synaptic o apt-get. Kubuntu 6.10 viene fornito con il pacchetto '**samba-common**' installato in modo predefinito, ma SAMBA non è né

completamente installato né configurato, pertanto avrete bisogno di scaricare i pacchetti.

Installare i pacchetti

Installare i pacchetti **samba** e **samba-doc** (con samba-doc si possono apprendere gli strumenti utili per una impostazione ottimale di SAMBA).

Questi pacchetti aggiuntivi non sono indispensabili, ma li ho installati comunque: **komba2**, **smb4k**, **swat**.

Creare/impostare la password smb

Dovete impostare la password smb del vostro utente in modo che sia la stessa tra windows e linux, eseguendo il seguente comando alla riga di comando (finestra del terminale):

```
sudo smbpasswd -a bob
```

Quindi, inserite la vostra password. Nel nostro esempio, bob è la persona loggata che sta digitando il comando su una macchina chiamata bob-samba. Per eseguire il comando

sopra, a bob verrà chiesto di creare una password per un utente di nome bob. Questo nome utente deve essere lo stesso nome di login utilizzato per accedere al vostro computer Windows e Linux.

Creare/Modificare il file smbusers

Una volta impostata la password di smb, è necessario o modificare o creare il file smbusers

```
sudo nano /etc/samba/smbusers
```

Inserite quindi la vostra password. Nel file smbusers, modificare o aggiungere la riga seguente:

```
USERNAME = "network username"  
USERNAME = il nome che si intende  
utilizzare per accedere alla  
macchina.
```

Utilizzando bob come esempio, sarebbe così:
bob = "network username"

Salvate il file e uscite dal vostro editor testuale.

Modificate il file di configurazione `smb.conf`

```
sudo nano /etc/samba/smb.conf
```

Quindi inserite la vostra password. È possibile utilizzare un qualsiasi editor. Io uso nano, poiché è presente sia in Ubuntu che in Kubuntu.

Nel file `smb.conf`, fate le seguenti aggiunte: Cercate la sezione intitolata

`[global]`

Se le seguenti voci non esistono, aggiungetele. Se esse esistono e sono impostate diversamente, modificarle in questa maniera:

`workgroup = MSHOME`

Inserite il nome del vostro gruppo di lavoro al posto di MSHOME.

`netbios name = bob-samba`

Inserite il nome dell'host del vostro computer `*buntu`.

Scorrete fino a individuare la voce seguente:

`; security = user`

Togliete il punto e virgola (;) dalla voce e aggiungete la seguente riga direttamente sotto di esso

`username map = #/etc/samba/smbusers`

Scorrete fino alla sezione

`==== Share Definitions ===`

in quella sezione, cercate la voce chiamata

`[printers]`

Dopo l'ultima voce per le stampanti, immettete le informazioni per le vostre condivisioni.

Ho posto la mia unità condivisa dopo la sezione stampanti perché per me funziona, ma potete metterli in qualsiasi parte della sezione Share Definitions. Ho dato un nome a ciascuna delle mie condivisioni nel file `smb.conf` in modo da abbinare il nome del disco come compare nella cartella `/media/`. Vi consiglio di utilizzare questo metodo per ragioni di semplicità.

Potete copiare e incollare le seguenti voci, se lo desiderate. Basta essere sicuri di modificarle in modo da riflettere il nome dei propri drive e dei nomi utente

`# Le mie cartelle condivise`

`[DRIVE1]`

`#path = /media/DRIVE1/`

`#browseable = yes`

`#read only = no`

`#guest ok = no`

`#create mask = 064`

`#directory mask = 0755`

`#force user = USERNAME`

`#force group = USERNAME`

`[DRIVE2]`

`#path = /media/DRIVE2/`

`#browseable = yes`

`#read only = no`

`#guest ok = no`

`#create mask = 0644`

`#directory mask = 0755`

`#force user = USERNAME`

`#force group = USERNAME`

Al posto delle voci "USERNAME", impostate USERNAME allo stesso nome utente che utilizzate per accedere al sistema Windows e Linux. Il nome del gruppo dovrebbe essere lo stesso del gruppo che utilizzate per il vostro account su Linux. Una volta che tutti questi passaggi sono stati completati, si può provare ad avviare Samba e ad accedere alle condivisioni.

```
sudo testparm
```

Quindi inserite la vostra password. Riavviate Samba.

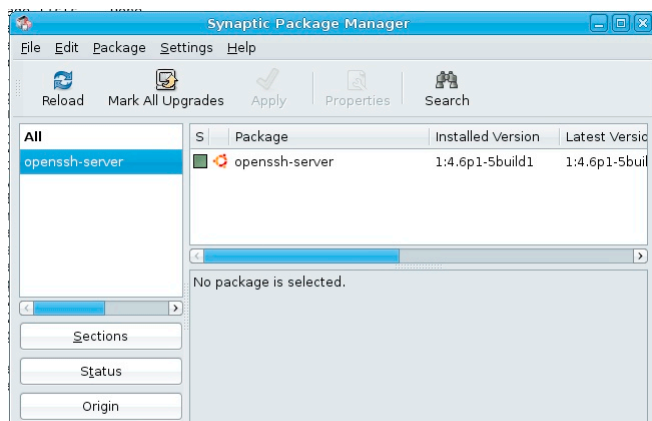
```
sudo /etc/init.d/samba restart
```

Inserite di nuovo la vostra password. Ora dovrete essere in grado di esplorare la rete dal tuo computer Windows e vedere/accedere/leggere/scrivere le condivisioni sul computer Linux. 🐧

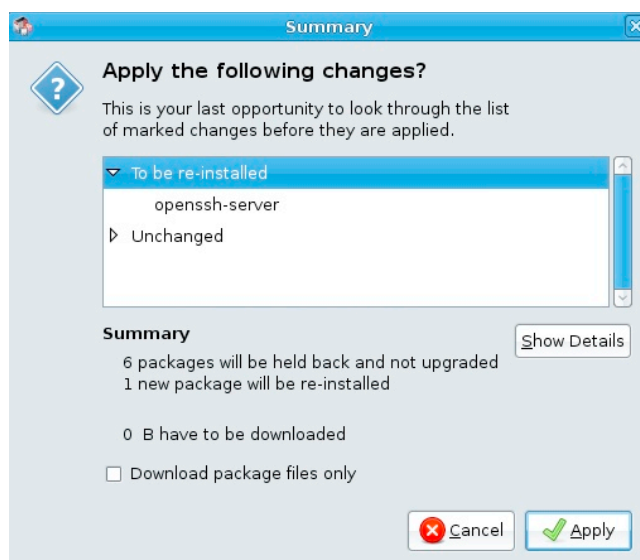
SSH (Secure Shell) è un protocollo che permette di connettersi in remoto da un altro computer su cui è installato un server SSH. L'interfaccia standard è un semplice linea di comando, anche se si possono eseguire applicazioni grafiche (X11) su un server Linux o BSD. Qui di seguito ci occuperemo della creazione di un client, del server, e del collegamento tra i due.

Come impostare un server

1 Avviate Synaptic (o Adept se usate Kubuntu) Sistema > Amministrazione > Gestore pacchetti Synaptic ed inserite la vostra password.



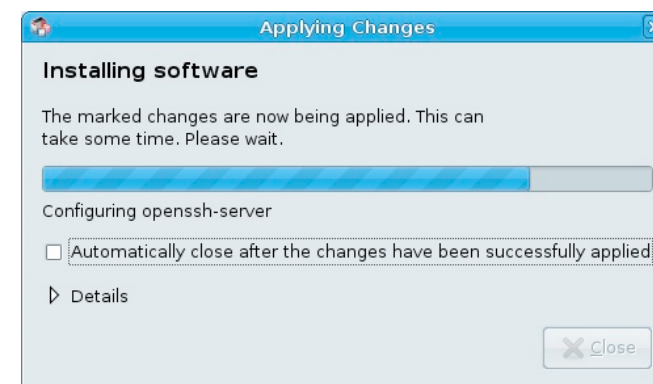
2 Cercate il pacchetto "openssh-server" e cliccate sulla casella vuota. Scegliete "Marca per l'installazione" dal menù.
3 Ripetete il passaggio precedente per il pacchetto "inadyn". (Sarà utile più tardi.)



4 Quando il programma vi mostra il seguente messaggio: "Applicare le seguenti modifiche?", Cliccate su "Applica".

5 Il pacchetto dovrebbe essere installato. Cliccate su "Chiudi" e uscite da Synaptic.

Finalmente avete un server installato! Vi



chiederete cosa potete fare con questo server. Beh, potete fare un bel po' di cose - da trasferimenti in remoto fino ad avviare applicazioni sul vostro computer da un altro. Prima di fare ciò però, c'è ancora qualche passaggio da completare. In primo luogo, dovete sapere come collegarvi al vostro computer da remoto. Dovete prima impostare un account DNS dinamico così potrete accedere al vostro computer tramite un sottodominio facile da ricordare, e non tramite un lungo indirizzo IP.

1. Andate sul sito web www.dyndns.com e fate clic su "Crea Account" sotto la casella del login nella parte superiore della pagina.
2. Scegliete un nome utente, password, e tutta

quella bella roba.

3. Confermate il vostro account per mezzo dell'email che vi è stata inviata ed effettuate il login.

Create Your DynDNS Account

Please complete the form to create your free DynDNS Account.

User Information

Username:		Instructions to activate your account will be sent to the e-mail address provided.
E-mail Address:		
Confirm E-mail Address:		Your password needs to be more than 5 characters and cannot be the same as your username. Do not choose a password that is a common word, or can otherwise be easily guessed.
Password:		
Confirm Password:		

About You (optional)

Providing this information will help us to better understand our customers, and tailor future offerings more accurately to your needs. Thanks for your help!

How did you hear about us:		We do not sell your account information to anyone, including your e-mail address.
Details:		

4. Fate clic sul collegamento "Miei servizi" e scegliete "Aggiungi il nuovo nome dell'host" sulla nuova pagina che vi si presenta.
5. Scegliete un nome dell'host, un sottodominio, e fate clic sul collegamento IP remoto riconosciuto automaticamente sotto il campo "Indirizzo IP". Fate clic su "Crea nuovo host".
6. Poi andate sul vostro terminale e digitate:

```
gksudo gedit /etc/crontab
```

premete il tasto invio e digitate la vostra password.

7. Digitate:

```
0 * * * * inadyd -u vostro_username -p
vostra_password -a
nome_che_avete_registrato > /dev/null
```

tutto su una sola riga. Non posso non sottolineare questo a sufficienza: non eliminate o cambiate alcunché.

8. Salvate ed uscite.
9. Adesso dovreste essere in grado di accedere al vostro computer entro circa un'ora tramite il dominio che avete registrato.

Per connettervi al vostro computer, digitate semplicemente:

```
ssh
[nomeutente]@[sottodominio.registrato]
```

da un terminale. La prima volta che vi connettete da una particolare macchina, potrete ottenere un messaggio del tipo

```
"L'autenticazione dell'host
[sottodominio] (indirizzo IP) non può
essere stabilita."
```

Potete tranquillamente ignorare questo messaggio, digitate "sì". Successivamente vi dovrebbe essere richiesta una password. Se inserita correttamente, dovreste essere al

prompt della linea di comando, sul vostro computer! Alcuni espedienti ingegnosi possono essere usati con SSH.

Eseguire applicazioni grafiche

Digitate:

```
ssh -X nomeutente@sottodominio
```

su un terminale. Inserite la vostra password come al solito, digitate il nome di un'applicazione grafica al prompt dei comandi (come "nautilus" o "thunar"). Vi si dovrebbe presentare sul computer che state usando se non è in esecuzione sul vostro computer.

Copiare file

Digitate:

```
scp
nomeutente@sottodominio:/percorso/al
/file nomeutente_del_computer_che_
state_usando@hostlocale:~/
```

e questo copierà il file dentro la vostra cartella home. 🔄

Spesso mi ritrovo a voler condividere i file tra il mio Pc principale e il mio portatile. Il piccolo disco rigido da 60GB del mio portatile non si presta bene a immagazzinare moltissimi file multimediali. La miglior soluzione che ho trovato è sshfs: esso combina la sicurezza di SSH con la semplice usabilità di un file system. Tutti i pacchetti richiesti sono disponibili nei repository di Ubuntu, così potreste aver bisogno di abilitare Universe e Multiverse.

In questo esempio sto utilizzando come “client” un portatile su cui è stato installato Gutsy Gibbon (questo è il PC che ho di fronte), mentre il “server” è un PC su cui è stato installato Dapper Drake (questo è il PC che ha i file a cui voglio accedere mentre sono seduto al portatile).

Utilizzando il vostro gestore di pacchetti preferito, installate questi pacchetti: tutto ciò di cui avete bisogno sul server è un server ssh (io utilizzo **openssh-server**). Sul lato client avrete bisogno di un client ssh (io utilizzo **openssh-client**). In aggiunta, avrete bisogno di **fuse-utils** e **sshfs**.

Un po' di lavoro dovrà essere fatto dalla linea di comando.

Prima di tutto aggiungetevi al gruppo “fuse” (sostituite username con la vostra *userid*):

```
sudo adduser username fuse
```

oppure andate su Sistema > Amministrazione > Utenti e Gruppi, fate clic su “Gestione Gruppi”, selezionate il gruppo *fuse*, fate clic su “Proprietà”, poi selezionate il box vicino alla vostra *userid* e fate clic su OK.

Successivamente avrete bisogno di cambiare i permessi di fusermount. Dalla vostra sessione di terminale:

```
sudo chmod 4755 /bin/fusermount
```

OK, questo è tutto per il setup. Ora iniziamo a utilizzarlo.

Prima di tutto effettuate un logout (non è necessario un riavvio) e fate nuovamente il login. Questo garantisce che tutti i processi del vostro utente abbiano i permessi di fuse che abbiamo appena assegnato. Ora create una cartella vuota dove volete (per esempio: `/home/user/mainpc`):

```
mkdir /home/user/mainpc
```

Anche se non è necessario, è più facile se aggiungiamo un accesso per *mainpc* nel file `/etc/host` del client. Quindi, per determinare l'indirizzo IP sul computer principale, eseguite su di esso:

```
ifconfig
```

L'output assomiglierà a qualcosa come questo (ho sottolineato la parte interessante):

```
eth0 Link encap:Ethernet HWaddr
      00:0D:87:A9:7E:3D
      inet addr:192.168.0.3
           Bcast:192.168.0.255
           Mask:255.255.255.0
      inet6 addr: fe80::20d:87ff:fea9:7e3d/64
           Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500
           Metric:1
      RX packets:50016073 errors:0 dropped:0
           overruns:0 frame:0
      TX packets:51997049 errors:0 dropped:0
           overruns:0 carrier:0
      collisions:0 txqueuelen:1000
```

```
RX bytes:2547247776 (2.3 GiB) TX
bytes:729954949 (696.1 MiB)
Interrupt:10 Base address:0xe000
```

Sul client editate il file `/etc/hosts` e aggiungete una linea simile a:

```
192.168.0.3 mainpc
```

Naturalmente utilizzerete l'indirizzo IP che avete trovato quando avete eseguito `ifconfig` sul PC principale.

Ora, montiamolo utilizzando `sshfs`:

```
sshfs
mainpc_user@mainpc://home/user/mainpc
```

Se non avessimo aggiunto `mainpc` al file `/etc/hosts`, allora avremmo avuto:

```
sshfs
mainpc_user@192.168.0.3://home/user/
mainpc
```

Ho montato il filesystem root di `mainpc`. Il client lo vede come `/home/user/mainpc`. Finché l'utente `mainpc` su `mainpc` ha accesso a qualcosa sul server, allora posso accedervi attraverso il punto di mount `/home/user/mainpc`. Non dovete montare / (potete montare la cartella a cui ha accesso l'utente `mainpc`).

Se utilizzate una porta alternativa a `ssh` (per esempio la 822 invece della 22 che è di default), allora il comando di mount assomiglierà a questo:

```
sshfs -p 822
mainpc_user@mainpc://home/user/mainpc
```

La mia rete wireless-G fornisce banda più che sufficiente per guardare un film su `sshfs`.

Come per quasi ogni altra utility, c'è sempre più di una scelta. La prima "perché non usate..." che viene in mente è Samba. Samba

ha la sua collocazione ma `sshfs` lo supera in tre categorie.

- Prima di tutto, `sshfs` fornisce automaticamente una comunicazione criptata attraverso `ssh`.
- In secondo luogo, mi permette di montare ogni cartella sul computer remoto senza riconfigurare.
- In terzo luogo, posso facilmente usare `sshfs` per montare un file system remoto tramite internet (non è necessario essere sulla mia rete locale).

Se state utilizzando un client Windows, allora Samba sarebbe la soluzione. Personalmente uso sia Samba che `sshfs`. 🐉

Avete mai avuto bisogno di un provvisorio access point (AP) Wi-Fi oppure di averne uno finché non potevate comprarvelo? Questo articolo vuole aiutarvi a crearne uno all'occorrenza.

Innanzitutto assicuratevi che la vostra scheda Wi-Fi sia pienamente supportata! Per esempio, alcune schede che usano Ndiswrapper potrebbero non funzionare. I passi da seguire potrebbero variare, quindi controllate questa pagina

<https://help.ubuntu.com/community/WifiDocs/WirelessCardsSupported>.

Per iniziare configureremo la vostra scheda Wi-Fi con una modalità ad-hoc in modo che si connetta direttamente via wireless a due o più computer senza l'uso di alcun router. Aprite il vostro terminale sull'AP (utilizzeremo questa sigla in tutto l'articolo) e digitate:

```
sudo iwconfig eth1 mode ad-hoc
```

Sostituite eth1 con l'interfaccia corretta della vostra scheda wireless. Per esempio, alcune schede sono ath0 o wifi0. Se non sapete

quale sia, potete lanciare il comando iwconfig che vi mostrerà qualcosa del genere:

```
ubuntu@server:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      unassociated  ESSID:off/any
          Mode:Managed  Channel=0  Access Point: Not-Associated
          Bit Rate:0 kb/s  Tx-Power=20 dBm  Sensitivity=8/0
          Retry limit:7  RTS thr:off  Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

In questo caso l'interfaccia sarebbe eth1. Quindi, configurate sulla scheda il canale su cui volete che l'AP sia attivo. Ho impostato il mio sul 4, che andrà bene per la maggior parte di voi. Fatelo digitando:

```
sudo iwconfig eth1 channel 4
```

Dopo ciò dobbiamo impostare un ESSID, cioè il nome dell'AP. Fatelo digitando:

```
sudo iwconfig eth1 essid APName
```

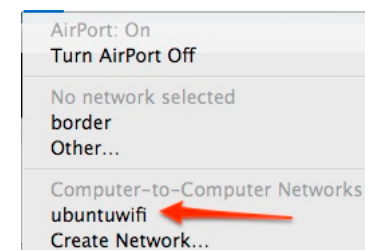
Abbiamo quasi finito. Se desiderate avere anche la cifratura per l'AP, potete aggiungere quella WEP digitando:

```
sudo iwconfig eth1 key abcde12345
```

Sostituite abcde12345 con la password scelta per la cifratura WEP.

Infine, date al vostro access point un indirizzo IP con:

```
sudo ifconfig eth1 169.254.xxx.xxx
```



Adesso, nel secondo computer, il client, verificate che il nuovo AP sia attivo.

Imposteremo anche un tunnel Secure Shell (SSH) su questo computer.

Creare un tunnel SSH

Anche se sto usando un Mac, funziona allo stesso modo su Linux.

Creare un tunnel SSH è abbastanza semplice: quello che dovete fare è generare una connessione SSH tra le due macchine.

Configurate il computer locale in modo da reindirizzare tutte le comunicazioni verso l'altra macchina attraverso quel tunnel. L'altra macchina si collega a internet e invia i dati. In questo caso, stiamo creando un tunnel SSH mediante una connessione ad-hoc (in genere ci dovrebbe essere soltanto un accesso wireless verso la seconda macchina, non a internet). Siccome l'altro computer è collegato a internet, possiamo far passare le comunicazioni in un tunnel mediante quella macchina e collegarci a internet in modalità wireless ma senza un router.

Per creare un tunnel, verificate che SSH sia avviato nell'AP (quello su cui abbiamo eseguito i comandi `iwconfig`). Tanto per essere sicuri digitate:

```
sudo /etc/init.d/sshd start
```

Ora, nell'altra macchina, il client (io sto usando un MacBook Pro), aprite un terminale. Ricordate che poco fa abbiamo assegnato all'altra macchina un indirizzo IP con `sudo`

`ifconfig eth1 169.254.xxx.xxx`? Ora ci serve. Digitate:

```
ssh -ND 9999 youruser@169.254.xxx.xxx
```

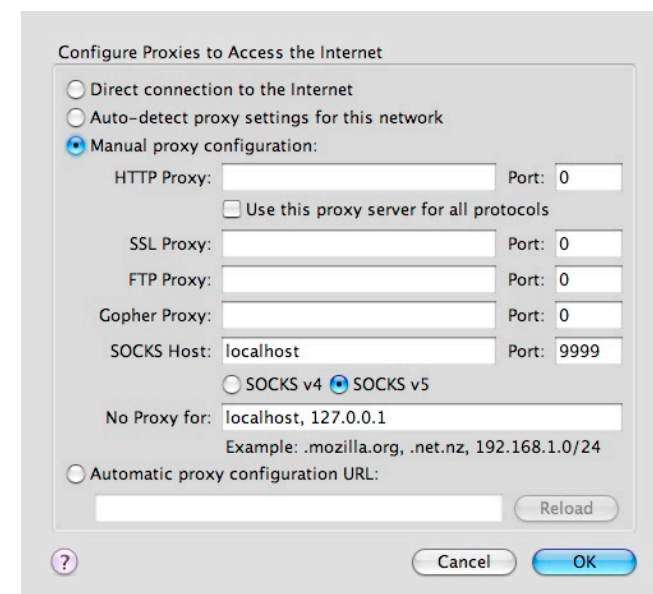
per avviare il proxy. SSH vi chiederà qualcosa del tipo:

L'autenticità dell'host 169.254.xxx.xxx non può essere stabilita. Siete sicuri di voler stabilire la connessione? (sì/no).

Rispondete "sì" e inserite la vostra password. Sembrerà che nulla sia successo, ma il vostro tunnel SSH è in funzione.

```
[~]$ ssh -ND 9000 ubuntu@169.254.92.13
The authenticity of host '169.254.92.13 (169.254.92.13)' can't be established.
RSA key fingerprint is a6:7f:7e:1f:7f:6d:59:8c:d0:7c:6e:27:90:97:15:9a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '169.254.92.13' (RSA) to the list of known hosts
ubuntu@169.254.92.13's password:
Permission denied, please try again.
ubuntu@169.254.92.13's password:
```

Infine avviate Firefox. Nelle preferenze andate nella scheda "Avanzate", quindi su "Rete" e fate clic su "Impostazioni". Fate clic su "Configurazione manuale dei proxy" e inserite



`localhost` nel campo "Host SOCKS". Digitate `9999` nel campo "Porta" di Host SOCKS.

Lasciate tutto il resto in bianco o con i settaggi predefiniti. Fate clic su OK.

Dovreste essere in grado di navigare sul web senza cavi!

Per ulteriori informazioni, leggete

<https://help.ubuntu.com/community/WifiDocs/Adhoc>. 

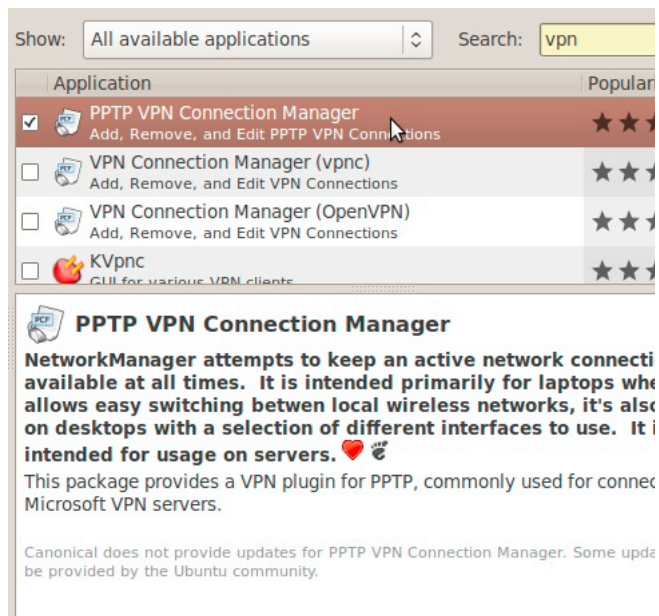
In una lettera nel numero 27 di FCM Ken ha richiesto alcune informazioni sulle VPN. Il mio articolo nel numero 2 riguardava l'utilizzo delle VPN, quindi ho pensato che fosse opportuno aggiornarlo visto che le cose ora sono cambiate.

Per prima cosa bisogna impostare le VPN attraverso il Network Manager. La maggior parte delle VPN che l'utente imposta utilizzano il protocollo PPTP. Il PPTP gira sulla porta TCP numero 1723. È necessario abilitare le porte in uscita dalla macchina locale o dalla LAN se bloccate. La maggior parte delle volte, ad esclusione dei maniaci della sicurezza che le bloccano, queste porte sono abilitate in uscita.

È necessario localizzare l'icona del Network Manager nell'area di notifica (potrebbe apparire in diversi modi): vi aiuta nell'effettuare le impostazioni della propria rete e iniziare le connessioni VPN.

Installiamo il modulo PPT in modo da iniziare la creazione delle connessioni VPN. Indovinate un po'? Non è più necessario

utilizzare la riga di comando (CLI) per farlo. Il PPTP è stato inserito nell'elenco delle applicazioni in Aggiungi/Rimuovi. Questo rende le cose semplici per coloro che non amano la riga di comando. Accedere ad Aggiungi/Rimuovi applicazioni e cercare VPN. Se si ordina la lista in base ai più popolari dovrebbe essere all'inizio. Spuntare la casella, applicare i cambiamenti, inserire la password, e fare clic su chiudi. Piuttosto semplice.

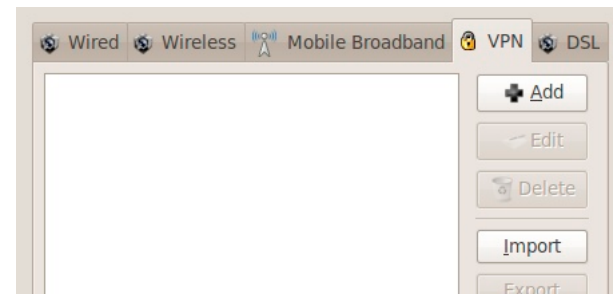


Per coloro che preferiscono la riga di comando possono utilizzare il seguente comando per installare i pacchetti necessari:

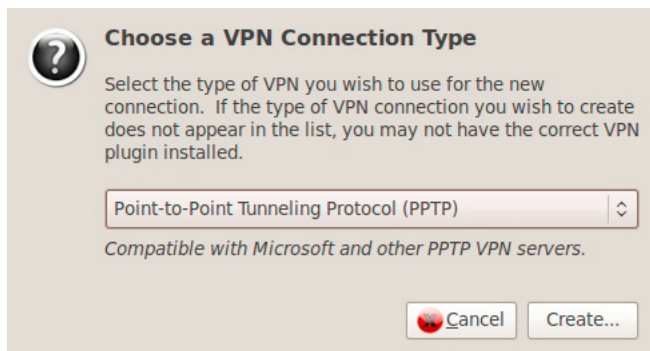
```
sudo aptitude install network-manager-pptp
```

Ora che il modulo PPTP è installato per il vostro Network Manager bisogna impostare la connessione. Fare clic con il pulsante destro del mouse su Network Manager nell'area di notifica e un menu contestuale si aprirà. Nel menu contestuale fare clic su Modifica Connessioni. Nota: è anche possibile fare clic sull'icona, andare in Connessioni VPN, e poi Configura VPN.

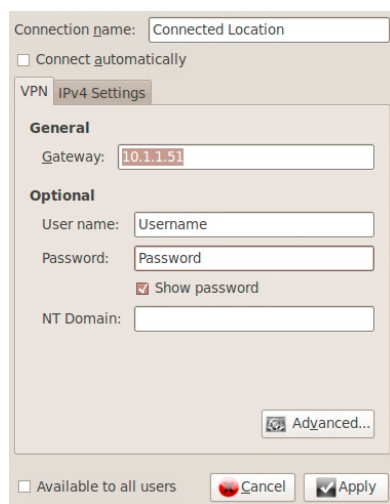
Nella finestra delle Connessioni di Rete fare clic sulla scheda VPN.



Di seguito fare clic su Aggiungi e poi su Crea.

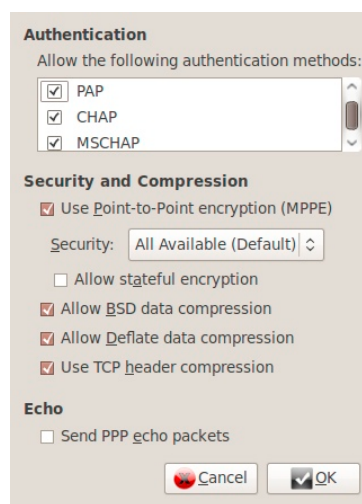


Modificare il nome della connessione. È possibile inserire qualsiasi nome, ma se si pensa di fare più di una connessione o se si hanno problemi a ricordare cosa si è inserito a distanza di 6 mesi, è una buona idea inserire il nome del luogo a cui ci si connette.

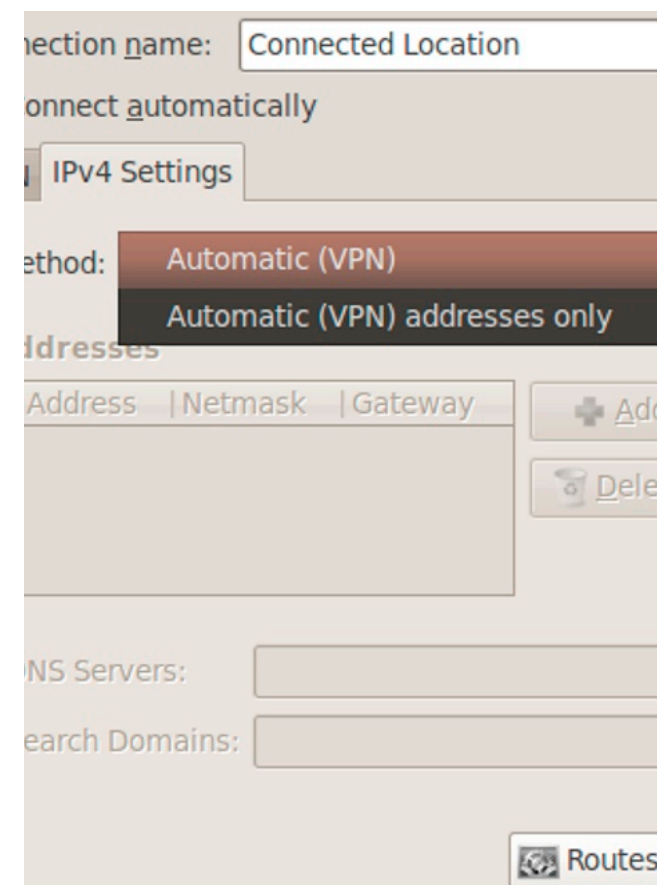


Nelle impostazioni del Gateway inserire l'IP o il FQDN (nome di dominio pienamente qualificato) a cui ci si connette. Personalmente, inserisco l'IP. Poi il nome utente. Generalmente non inserisco una password, credo sia semplicemente una buona abitudine. Dipende dall'utente se inserire una password o meno. Se volete inserire la password, questa dovrebbe essere legata al portachiavi.

Potrebbe essere necessario andare nella sezione Avanzate per selezionare la cifratura. Potrebbe essere necessario spuntare il Usa cifratura Point-to-Point (MPPE) per connettersi. La maggior parte delle VPN richiedono una connessione cifrata. Fare clic su OK.



La scheda delle Impostazioni IPv4 è rivolta ad utenti esperti. Qui si possono cambiare i server DNS per il vostro VPN, impostare diversi instradamenti di rete basati su sottorete e assegnare un IP statico. Le cose dovrebbero funzionare senza la necessità di trafficare con la scheda delle impostazioni di IPv4. 🚫





Programmazione

Compilare da sorgente

Creare e distribuire file .deb



Ubuntu vanta un repository di pacchetti molto vasto. Malgrado ciò a volte un pacchetto può non essere disponibile oppure potreste aver bisogno di compilarlo da sorgente: per farlo sono necessari pochi semplici comandi. Per compilare da sorgente, effettuate i seguenti passi.

Per compilare i pacchetti, è necessario il pacchetto **build-essential**, che può essere installato semplicemente con il comando:

```
sudo apt-get install build-essential
checkinstall
```

Altrimenti, se apt-get non vi piace, installate **build-essential** e **checkinstall** utilizzando un gestore di pacchetti a vostra scelta.

Ora dovete decomprimere l'archivio contenente il codice sorgente. Nel caso di un

file `.tar.gz` potete farlo con:

```
tar -xvzf example.tar.gz
```

Dove `esempio.tar.gz` è il nome del file. Se invece avete un file zippato (`.zip`), utilizzate il comando seguente:

```
unzip file.zip
```

La directory dove vi trovate attualmente all'interno del terminale è il luogo in cui sarà estratto l'archivio. Ora che lo avete estratto, fate `cd` verso la directory principale dell'archivio con:

```
cd /percorso-directory
```

E digitate il comando seguente:

```
./configure
```

Successivamente, digitate:

```
make
```

Infine, digitate:

```
sudo make install
```

Se volete compilare un file Debian (`.deb`), digitate:

```
sudo checkinstall
```

Quest'ultimo dovrebbe quindi fornirvi una comoda procedura guidata per l'installazione dei sorgenti simile a quanto esposto sopra. A questo punto avete compilato ed installato i sorgenti. Se avete problemi, potete chiedere aiuto in qualsiasi momento su UbuntuForums.org, oppure sul canale IRC di Ubuntu.

Quasi tutti sanno cos'è un pacchetto .deb. È l'“installer” per Ubuntu, Debian, MEPIS e molte altre distribuzioni Linux. A mio parere, il miglior formato disponibile per distribuire applicazioni. Sfortunatamente, molti programmi Linux non includono un archivio .deb, ma viene fornito solo il codice sorgente, che spesso richiede lo scaricamento di una serie di librerie aggiuntive che non avete mai sentito (il cosiddetto “inferno delle dipendenze”), e il più delle volte non comprende neppure l'opzione per disinstallare il programma. Tuttavia, creare un pacchetto .deb da zero è più facile di quanto crediate.

CheckInstall e Debian Package Tools FE

Il metodo più semplice (e peggiore) è utilizzare un programma di pacchettizzazione .deb chiamato [checkinstall](#). A prima vista può sembrare eccezionale: tutto quello che c'è da fare è eseguire il comando `make` (come d'abitudine) per compilare il codice sorgente e quindi eseguire `checkinstall` per creare il file .deb. Purtroppo sorgono numerosi problemi, primo fra tutti, le dipendenze non vengono

installate (potete provare [AutoApt](#) o [AutoDeb](#), entrambi sperimentali) né è possibile dichiararle, obbligando gli altri utenti ad installarle manualmente per far funzionare il programma. Dunque, per creare pacchetti di qualità, CheckInstall non rappresenta la strada ideale. Se, d'altra parte, siete interessati a creare pacchetti semplici senza troppe seccature, CheckInstall può esservi utile. Comunque, non mi occuperò di CheckInstall in questo articolo (potete trovare un tutorial al seguente indirizzo: <https://help.ubuntu.com/community/CheckInstall>).

C'è quindi qualche altro semplice metodo per creare pacchetti di qualità?

Esiste Debian Package Tools FE (<http://url.fullcirclemagazine.org/927dc1>), un'applicazione basata sulle librerie Qt, che fornisce un'interfaccia grafica semplice per la creazione di pacchetti. È molto meglio di CheckInstall, ma non rappresenta ancora il metodo ideale per creare pacchetti di qualità.

Creazione manuale dei pacchetti

Il primo passo per la creazione manuale degli archivi .deb è scaricare il programma, quindi compilarlo (se necessario) ed installarlo. Questo solitamente comporta eseguire nell'ordine `./configure`, `make`, e `sudo make install`. A questo punto trovate dove è stato installato, aprite il file Makefile con un editor di testo e leggete la sezione `install`, se non lo trovate, cercate nella cartella `/usr/`. Ora è tempo di creare il file di controllo, fondamentalmente, si tratta della descrizione del .deb. Ecco un esempio di file di controllo (dovete copiare tutto in un file chiamato “control”, senza estensione):

```
Package: fungame
Version: 1.0
Section: games
Priority: optional
Architecture: i386
Essential: no
Depends: libfungame, gamelibrary (>=
1.4.0)
Recommends: fungamesaves1 |
fungamesaves2
Suggests: optionalfungame
```

```

Installed-Size: 1024
Maintainer: Game Maker
    [gamer@gamers.net]
Conflicts:
    stupidfungamethatbreaksthisone
Replaces: oldfungame
Description: A short description of the
    program
.
A longer description

```

Notate alcune cose. Primo, è necessaria una linea vuota alla fine del testo, è fondamentale, se non viene lasciata il .deb. non funzionerà. I campi sono abbastanza ovvii.

- Il campo **Package** contiene il nome del pacchetto, se il nome del vostro pacchetto contiene più parole utilizzate un trattino (-) tra di esse. I nomi dei pacchetti possono contenere solo lettere minuscole, numeri e (credeteci o no) "+" e "-".
- La sezione **Version** è ovviamente la versione del programma, assicuratevi solo che non contenga dei trattini (-).
- La voce **Section** è una lista di categorie a cui appartiene l'applicazione, tra cui admin, games, gnome, kde, mail, misc, net, sound, text, utils e web.
- La chiave **Priority** indica la priorità del programma, il più delle volte opzionale.

- **Architecture** è l'architettura del computer su cui gira il programma, solitamente i386, AMD64 o PowerPC.
- **Essential** indica se si tratta di un programma fondamentale o no, di solito no.
- **Depends, Recommends, e Suggests** invece sono tutti simili: *Depends* indica che il nostro programma non funzionerà senza quella dipendenza, *Recommends* contiene indicazioni su quanto possa essere utile al nostro programma per funzionare, ma non obbligatori, e *Suggests* identifica tutto ciò che sarebbe carino avere in aggiunta. Potete indicare le varie dipendenze separate da una virgola (,), mentre se è necessario indicare più programmi alternativi potete separarli con un una linea verticale (|). Potete anche aggiungere, tra parentesi, la versione da utilizzare, indicando << (precedente), <= (precedente o uguale a), = (uguale a), >= (successiva o uguale a) oppure >> (successiva).
- **Installed-Size** è la dimensione in kilobyte del file installato.
- **Maintainer** siete voi (il vostro nome seguito dall'indirizzo di posta elettronica tra parentesi quadre []).
- **Conflicts** mostra i pacchetti che impediscono l'installazione del programma (programmi che vanno in conflitto con

l'applicazione).

- **Replaces** contiene la lista dei pacchetti che verranno rimpiazzati dal vostro applicativo.
- Per ultimo, **Description** contiene la descrizione del software.

Una volta preparato il file di controllo, salvatelo in una cartella /DEBIAN. Ad esempio, se state creando un pacchetto e la cartella di lavoro è ~/fungame/, salverete il vostro file di controllo in ~/fungame/DEBIAN/.

È ora il momento di aggiungere il programma vero e proprio, copiandolo nella cartella di lavoro. Ad esempio, se fungame è presente in /usr/local/fungame/ e come file binario in /usr/bin/fungame e la vostra cartella .deb è ~/fungame/, copiate tutto il contenuto di /usr/local/fungame/ in ~/fungame/usr/local/fungame/ e /usr/bin/fungame in ~/fungame/usr/bin. Potete anche creare una voce di menù (un file .desktop) in ~/fungame/usr/share/applications/fungame.desktop, ecco un esempio di file .desktop:

```

[Desktop Entry]
Type=Application
Version=1.0

```

```

Encoding=UTF-8
Name=Fun Game
Exec=fungame
Comment=
Icon=/usr/local/fungame/fungame.png
Terminal=false
Categories=Application;Game;
StartupNotify=false
MimeType=

```

Se volete, potete omettere la linea `Icon=`.

Ora, è finalmente tempo di creare il vostro archivio. Per fare questo, fate `cd` nella cartella di lavoro (ad es. `~/fungame/`) ed eseguite in un terminale

```
run dpkg -b cartella nomepacchetto.deb
```

dove `cartella` è la vostra directory, ad es. `~/fungame/`, e `nomepacchetto.deb` è il nome dell'archivio che volete creare. È importante nominare correttamente il pacchetto secondo la seguente convenzione: `nome-programma_versione_architettura.deb`. Tutto deve corrispondere all'equivalente presente nel file di controllo.

Distribuire il pacchetto

Il vostro pacchetto riceverà massima attenzione se disponibile su packages.debian.org e packages.ubuntu.com. Purtroppo non potete fare un semplice upload, ma dovete essere sviluppatori Debian (oppure Ubuntu) e diventarlo non è un processo semplice. Un lungo articolo sull'argomento è disponibile su

<http://www.linux.com/articles/42155>. Un metodo più semplice è quello di trovare un mentore che si occupi di caricare il file per voi (si veda <http://mentors.debian.net/>). Quindi, cosa si può fare se non si vogliono aspettare i lunghi tempi di registrazione come sviluppatore Debian/Ubuntu? Se avete letto la mia classifica Top5, sapete che adoro GetDeb.net. Questo sito fornisce file `.deb` di terze parti e rappresenta il posto ideale per programmatori non-Debian e non-Ubuntu che vogliono fornire i propri pacchetti. Potete trovare le istruzioni per farlo al seguente indirizzo: http://wiki.getdeb.net/Building_Packages. Soprattutto non è richiesta nessuna registrazione, ma solo un account su Launchpad.net. 



Multimedia

Convertire un DVD con AcidRip

Creare una macchina MAME



Ne so ben poco di compressione video, ma ho comprato di recente un MediaPlayer Freecom che si collega direttamente al televisore e mi permette di guardare file video e ascoltare musica. Inoltre volevo anche guardare i video della mia famiglia sul mio piccolo lettore multimediale nuovo. Ho circa una dozzina di DVD autoprodotti e ognuno di essi è piuttosto grande (3-4 Gb). Volevo comprimere questi video per gestire meglio lo spazio sul mio lettore multimediale. Per comprimerli, ho deciso di usare AcidRip.

Per installare AcidRip, fate clic su Sistema > Amministrazione > Gestione dei pacchetti Synaptic. Dalla barra dei menu di Synaptic, fate clic su Impostazioni > Repository ed assicuratevi che il repository multiverse (Software vincolato da copyright oppure da azioni legali) sia selezionato. Fate clic su "Chiudi" per chiudere la finestra "Repository". Successivamente fate clic sul tasto "Reload" sulla barra degli strumenti di Synaptic per assicurarvi di avere a disposizione l'ultima versione del software. Fate clic sul pulsante "Cerca" nella barra degli

strumenti di Synaptic e cercate "acidrip". Quando compariranno i risultati, vedrete AcidRip e sarà possibile fare doppio clic su "AcidRip" per selezionarlo per l'installazione.

Successivamente fate clic sul pulsante "Applica" sulla barra degli strumenti di Synaptic per installare il software.

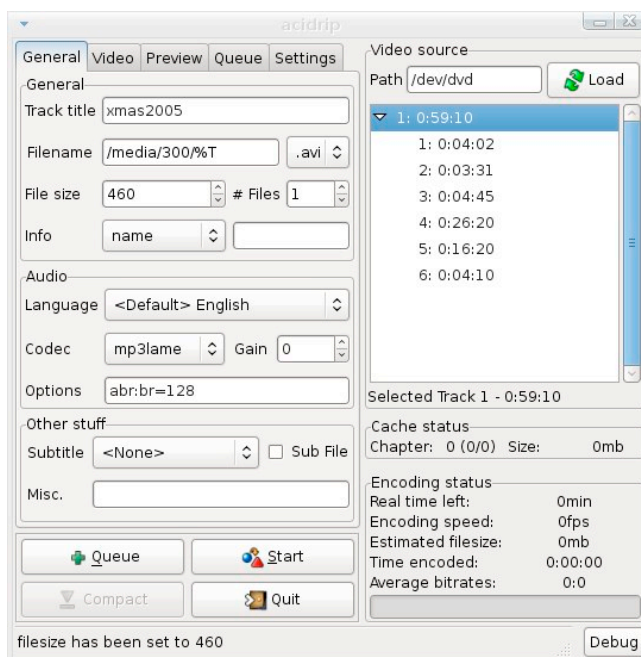


Figura 1 (sopra): Impostazioni Generali di AcidRip

Eseguire AcidRip

Dopo l'installazione, eseguite AcidRip da Applicazioni > Suoni & Video > AcidRip > DVD Ripper. Dopo aver lanciato AcidRip, verrà visualizzata la finestra principale, come in Figura 1 (sinistra). Inizialmente le opzioni sembreranno davvero troppe, ma per cominciare dovrete inserire il DVD nell'apposito cassetto e fare clic sul pulsante "Carica" per accedere ai contenuti del DVD. Come si vede in basso, il DVD dell'esempio è stato caricato con il titolo "xmas2005", con 6 capitoli e durata di circa 59 minuti. Ho specificato manualmente l'impostazione "Nome file" dal valore di default "/home/jonny/%T" a "/media/300/%T" in modo tale che il video finale compresso verrà salvato come xmas2005.avi sul dispositivo esterno di 300 GiB montato precedentemente nel percorso /media/300. Ho anche cambiato il valore predefinito di "Dimensione file" da 700 a 460 in modo da avere un file di 460 megabyte (MiB).

Consiglio: Dopo aver cambiato la dimensione del file, fate clic su un altro campo nella

finestra (es. il campo Titolo della Traccia) per assicurarvi che i cambiamenti fatti siano salvati. Se non effettuate quest'operazione, il cambiamento non verrà notato da AcidRip - probabilmente un piccolo bug.

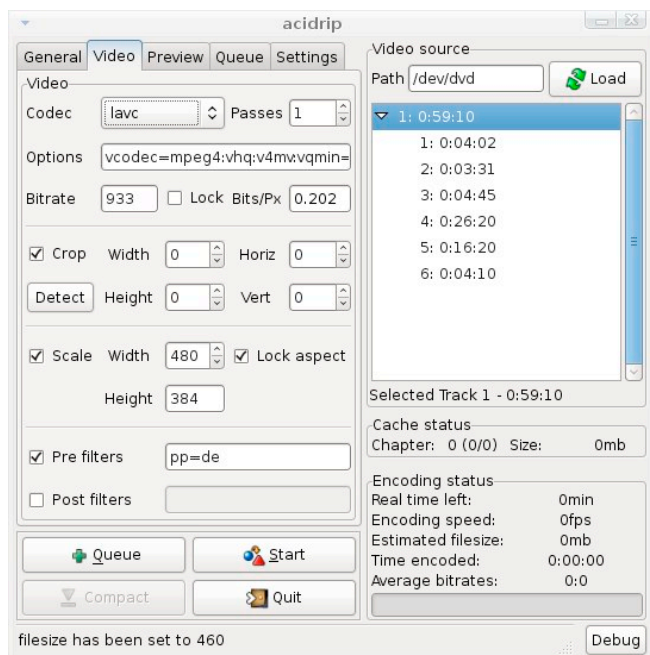
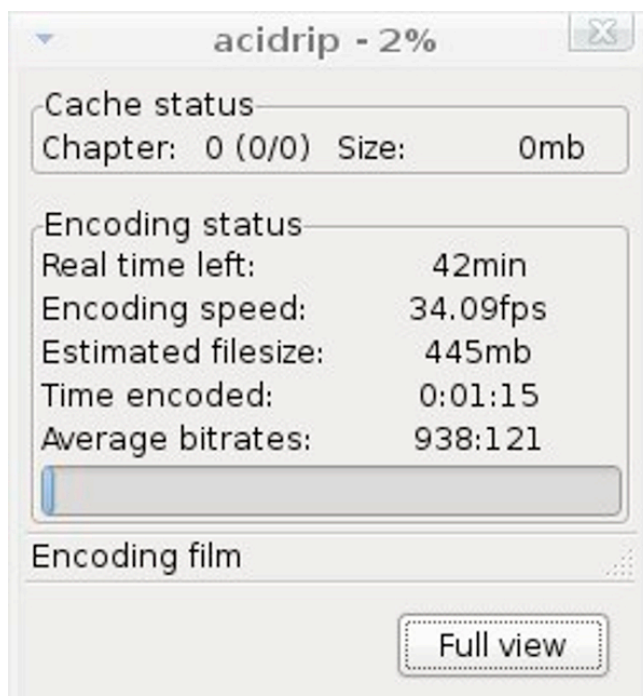


Figura 2 (sopra): Impostazioni Video di AcidRip

La dimensione di 460 MiB è adatta per un video di un'ora, mentre 700Mb sarebbero giusti per un video di 90 minuti.

Per cominciare il vero processo di conversione, fate clic sul pulsante "Start" in basso alla finestra di AcidRip. La finestra di AcidRip principale scomparirà ed apparirà una finestra con una barra progressiva, come questa in basso.



Dopo che la conversione (sopra) avrà raggiunto il 100%, accederete nuovamente alla finestra principale di AcidRip (figura 1). A questo punto, sarà possibile aprire il

Navigatore di File (Luoghi > Home) e trovare il nuovo video compresso pronto per essere guardato.

In conclusione

Ci sono diverse alternative per convertire i DVD, come per esempio DVD::rip (sotto) che mi sembra un po' complicato e Thoggen, leggermente più lento, ma se si vuole convertire velocemente e senza problemi, AcidRip supera certamente il mio "acid test".



MAME è un'applicazione chiamata *Multiple Arcade Machine Emulator* (NdT: Emulatore di Macchine Arcade Multiple). In breve, gli fornisce delle ROM di vecchie macchine *arcade* e lui le avvia. MAME di per sé non è così comodo da utilizzare o vedere, così la maggior parte delle persone utilizza un'applicazione grafica che permette un accesso più semplice alle proprie ROM. Io utilizzo Ubuntu 8.10 come sistema operativo e utilizzerò **Wahcade** come interfaccia per MAME. La mia idea è quella di avere il mio vecchio PC collegato alla TV utilizzando la presa uscita TV della scheda video.

Installare Ubuntu

Installare Ubuntu su di un PC è semplice. O meglio, normalmente è così. Visto che non utilizzo un monitor, Ubuntu non può determinare la risoluzione, ma il rinnovato X, festoso e a prova di proiettile, mi viene in aiuto e mi permette (alla fine) di caricare Ubuntu in bassa risoluzione (800x600) che è sufficiente per farmi andare avanti.

TRUCCO: Se dovrete utilizzare il PC solo per

MAME vi conviene selezionare l'accesso automatico nel passo 5 dell'installazione. Scoprirete il perchè alla fine di questo articolo.

Con Ubuntu installato, ora è necessario installare tutti gli ultimi aggiornamenti, tutti i 200 e più! Ma una volta sistemati gli aggiornamenti, ho accesso ai driver proprietari nVidia e posso configurare opportunamente l'uscita TV della scheda video.

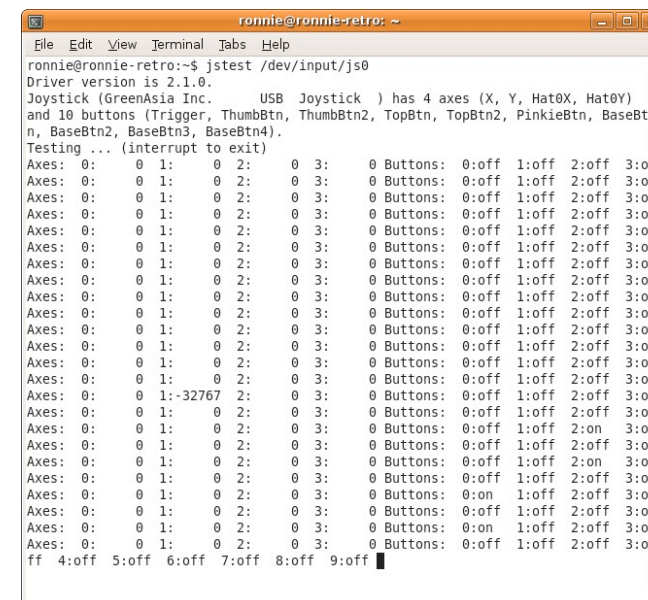
Ubuntu è installato, ma gli piacerà il mio joypad economico Logic3? È ora di scoprirlo. Ho installato il pacchetto **joypad** utilizzando Synaptic. Dalla riga di comando ho avviato:

```
jstest /dev/input/js0
```

Nota: alcune distribuzioni potrebbero utilizzare `/dev/js0`

Ciò permette di testare tutti i movimenti e i bottoni del joypad (fig. in alto a destra).

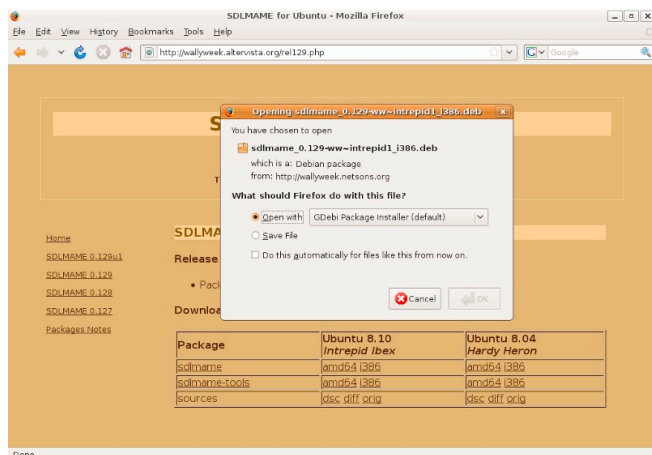
Questo conferma che il joypad è riconosciuto e interamente funzionante. Eccellente!



```
ronnie@ronnie-retro: ~  
File Edit View Terminal Tabs Help  
ronnie@ronnie-retro:~$ jstest /dev/input/js0  
Driver version is 2.1.0.  
Joystick (GreenAsia Inc. USB Joystick ) has 4 axes (X, Y, Hat0X, Hat0Y)  
and 10 buttons (Trigger, ThumbBtn, ThumbBtn2, TopBtn, TopBtn2, PinkieBtn, BaseB  
tn, BaseBtn2, BaseBtn3, BaseBtn4).  
Testing ... (interrupt to exit)  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
Axes: 0: 0 1: 0 2: 0 3: 0 Buttons: 0:off 1:off 2:off 3:0  
ff 4:off 5:off 6:off 7:off 8:off 9:off
```

MAME!

Ora vediamo di installare **SDLmame**. Il sito <http://wallyweek.altervista.org/> ha un file .deb da scaricare. Selezionate semplicemente il collegamento corretto e, quando Firefox vi mostrerà una finestra per chiedervi se volete salvare il file, sarà presente anche un'opzione per aprire il file con Gdebi. Io utilizzo questa opzione perchè risparmia tempo scaricandolo e avviandolo con un solo click:



È esattamente la stessa idea per scaricare **Wahcade**:

<http://www.anti-particle.com/wahcade.shtml>

Con Sdlmame e Wahcade installati, siamo pronti a rockeggiare!

/Home nelle vicinanze

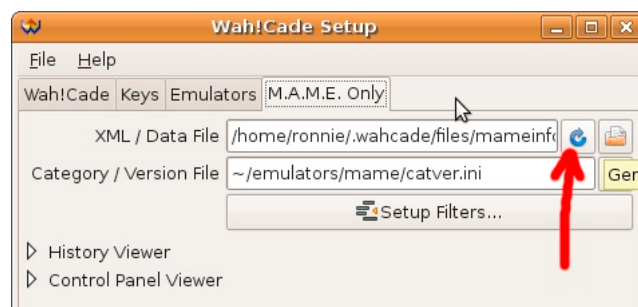
Nella vostra cartella /home create una directory chiamata `emulators`, all'interno della quale ne creerete una chiamata `mame`, al cui interno ne creerete una chiamata `roms`. Questo è il percorso predefinito per Wahcade e semplifica la sua configurazione.

Configurazione

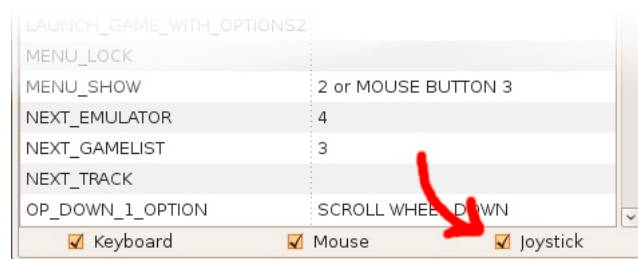
Se controllate il menu Applicazioni > Giochi

vedrete alcune voci per Wahcade. Per il momento vogliamo avviare l'applicazione di configurazione. Le uniche cose che dobbiamo editare sono: nella scheda Emulators (a sinistra), aprete la voce List Generation, premete sfoglia e selezionate la cartella `roms` (`/home/vostronome/emulators/mame/roms`).

Nella scheda MAME Only premete il pulsante per generare una lista delle vostre ROM:



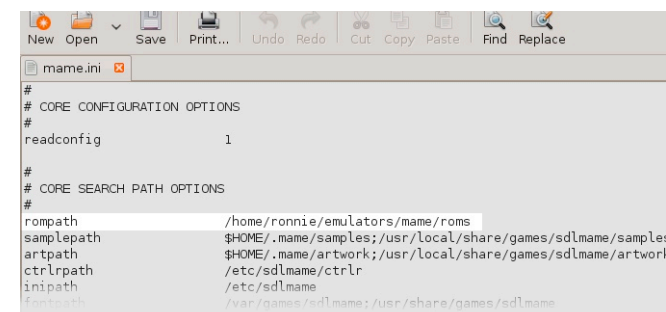
E infine, la scheda Keys. Probabilmente non dovrete modificare niente qui, ma io devo selezionare l'opzione per abilitare il mio joystick a selezionare le ROM in Wahcade:



L'ultima cosa da configurare è Sdlmame stesso. Ha bisogno di conoscere dove sono nascoste le vostre ROM. Quindi da terminale, scrivete:

```
sudo gedit /etc/sdlmame/mame.ini
```

Dove dice `rompath`, copiate/scrivete il percorso della cartella con le ROM (la stessa che avete definito in Wahcade).



È tempo di fare una prova! Andate su Applicazioni > Giochi e avviate Wahcade!





Super Sprint (rev 4)

SSPRINT

1986 Atari Games

0 Raster

Status Good, Color Good, Sound Good



All Games

Super Space 2001
Super Speed Race
Super Sprint (French)
Super Sprint (German, rev 1)
Super Sprint (German, rev 2)
Super Sprint (Spanish)
Super Sprint (rev 1)
Super Sprint (rev 3)
Super Sprint (rev 4)

Il tema predefinito di Wahcade è abbastanza vistoso, ma altri possono essere scaricati da numerosi siti. Anche io ho creato un semplice layout MAME (a sinistra) per Wahcade: http://ronnietucker.co.uk/mame/polaroid_1024.zip

La ragione per abilitare l'accesso automatico in Ubuntu è che potete andare in Sistema > Preferenze > Sessioni e aggiungere Wahcade all'avvio. Questo significa che la vostra macchina MAME caricherà Ubuntu, eseguirà l'accesso e avvierà Wahcade per voi. Vi sconsiglio di utilizzare l'accesso automatico se la vostra macchina dovrà essere usata per qualsiasi altra cosa! Non solo, ma Wahcade può essere utilizzato come interfaccia grafica per la maggior parte degli emulatori, quindi in realtà potrete avere questa interfaccia per tutti i vostri emulatori e anche avere differenti temi di Wahcade per ciascun emulatore! 🎮



Sicurezza

TrueCrypt su Ubuntu

Tenere al sicuro i bambini in Linux



Almeno una volta al mese leggiamo sul giornale che un portatile importante è stato rubato. Veniamo a scoprire poi che questo portatile conteneva i nomi di ventimila impiegati o clienti, compresi numeri di sicurezza sociale, numeri di conti bancari e altre informazioni riservate. Ridiamo tra di noi pensando che certamente mai faremmo una cosa così stupida come lasciare informazioni personali e riservate pronte per essere raccolte da qualunque malintenzionato. Giusto? Forse no. Il vostro portatile è veramente protetto di modo che, se venisse rubato, nessuna informazione riservata potrebbe essere raccolta?

Il mio portatile contiene tutte le registrazioni finanziarie di casa, compresi numeri di conto, informazioni di accesso con password, ecc. Tengo anche le password per altri account online. In più, conservo copie delle lettere personali che ho spedito in passato. Tutte queste informazioni sono molto riservate e sicuramente non voglio che finiscano nelle mani di un malintenzionato. Dunque come si possono proteggere queste

informazioni senza spendere troppo tempo e fatica?

La risposta, naturalmente, sta in un software chiamato TrueCrypt. Il testo che segue è tratto dalla introduzione alla Guida utente di TrueCrypt:

"TrueCrypt è un sistema software per creare e mantenere un volume (dispositivo di archiviazione dati) cifrato al volo. Per cifratura al volo si intende che i dati sono cifrati e decifrati automaticamente poco prima di essere caricati o salvati, senza alcun intervento da parte dell'utente. Nessun dato archiviato su un volume cifrato può essere letto (decifrato) senza l'uso della corretta password/keyfile o delle corrette chiavi di cifratura. L'intero filesystem viene cifrato (ad esempio, i nomi dei file, i nomi delle cartelle, i contenuti di ogni file, lo spazio libero, i metadati, ecc.). I file possono essere copiati in e da un volume di TrueCrypt montato proprio come quando vengono copiati in e da un qualunque altro normale disco (per esempio, con semplici operazioni di drag-and-drop). I file vengono automaticamente decifrati al

volo (nella memoria RAM) mentre vengono letti o copiati da un volume di TrueCrypt montato. Allo stesso modo, i file scritti o copiati nel volume di TrueCrypt vengono automaticamente cifrati al volo (proprio prima di essere scritti nel disco) nella RAM."

Quando si crea un volume di TrueCrypt, in pratica si definisce e si crea un file (chiamato contenitore nella terminologia di TrueCrypt) che sarà montato come un filesystem. Si può accedere (cioè montare) al filesystem immettendo la password corretta. Da quel momento, si può accedere a qualunque file nel filesystem/contenitore come si farebbe con qualunque altro file in qualunque altro filesystem.

Il software fa molto più di questo; ha molte funzioni in più che vanno oltre lo scopo di questo articolo. Una funzione interessante è il "volume nascosto". Immaginiamo che siate forzati ad aprire il contenitore (qualcuno vi ha puntato una pistola). La funzione del volume nascosto vi permette di sbloccare il contenitore e mostrare al malvivente il volume sbloccato senza dirgli che lì c'è un

secondo volume (contenente i veri dati) nascosto sotto le coperte. Senza sapere che esiste, non si può dedurre la presenza. È utile spendere del tempo per leggere le 92 pagine del manuale utente distribuito col software.

TrueCrypt è disponibile per Linux come per Windows, sia in binario che in codice sorgente. Per installare TrueCrypt su Ubuntu, bisogna recarsi all'area download del sito di TrueCrypt:

<http://www.truecrypt.org/downloads.php>.

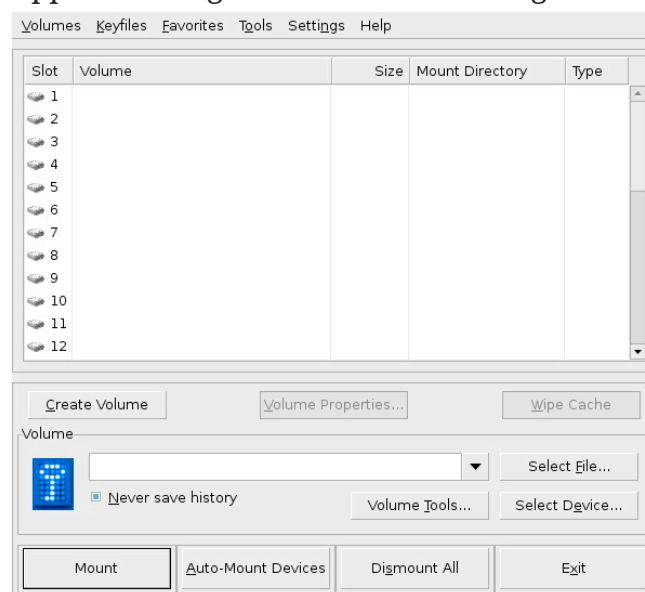
Andate nella sezione per Linux e scegliete "Ubuntu (x86)". Verrà scaricato il file `truecrypt-5.0-ubuntu-x86.tar.gz`. Per facilitarvi le cose, salvate il file sul desktop. Una volta salvato, fate doppio clic sull'icona del file; il gestore degli archivi di GNOME, File Roller, aprirà una finestra col contenuto di questo file tar.gz. Uno di questi file è `truecrypt_5.0-0_i386.deb`. Trascinate il file sul desktop e fate doppio clic sull'icona. Apparirà l'installer del pacchetto. Fate clic sul pulsante "Installa pacchetto" e rilassatevi un attimo mentre TrueCrypt si installa.

Finita l'installazione di TrueCrypt, creiamo un contenitore di TrueCrypt. Si tenga a mente che questo contenitore, quando impostato correttamente, apparirà come un filesystem

una volta che sarà stato montato. Avviate TrueCrypt aprendo un terminale (Applicazioni > Accessori > Terminale). Immettete il comando:

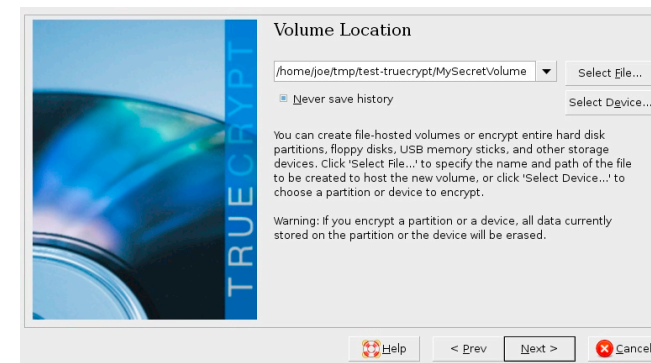
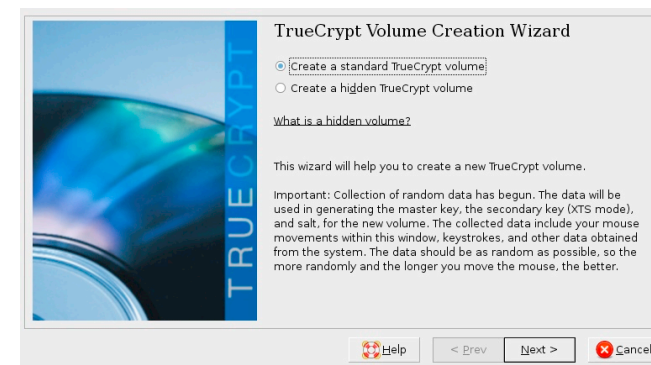
```
truecrypt
```

Apparirà la seguente finestra di dialogo:

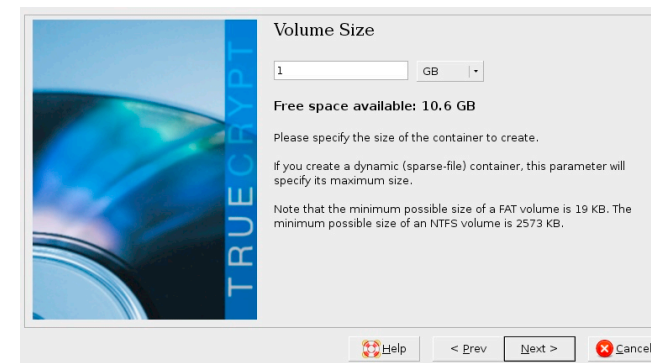


Dal menu selezionate Volumes > Create New Volume. Apparirà una seconda finestra di dialogo.

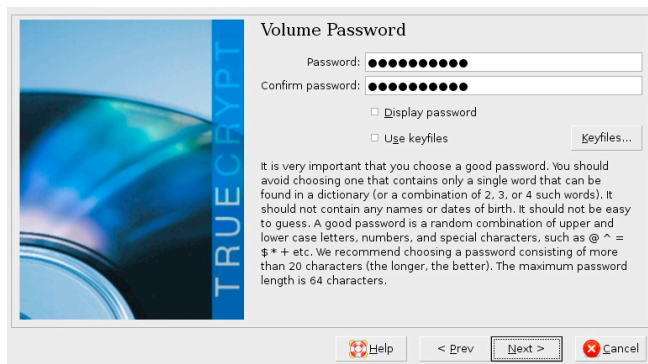
Fare clic su Next. Apparirà la terza finestra di dialogo. Immettete qui il nome del file che intendete creare per la gestione del filesystem cifrato. Quindi fate clic sul pulsante Next.



Vi verrà chiesta la dimensione del file-contenitore. Io ho scelto 1GiB.

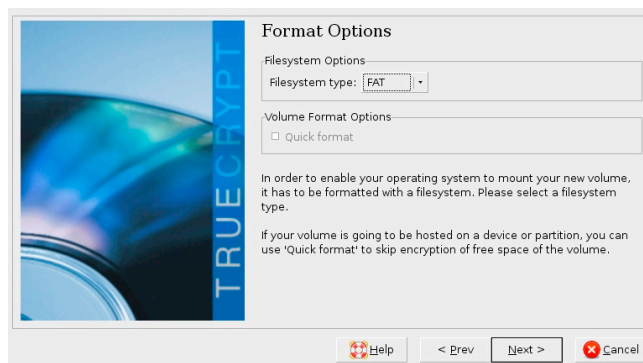


La finestra di dialogo successiva vi permette di scegliere quale algoritmo di cifratura utilizzare per la cifratura dei contenuti del contenitore. Potete informarvi sulle varie scelte leggendo la Guida Utente di TrueCrypt. Lasciate le scelte predefinite e fate clic sul pulsante Next.

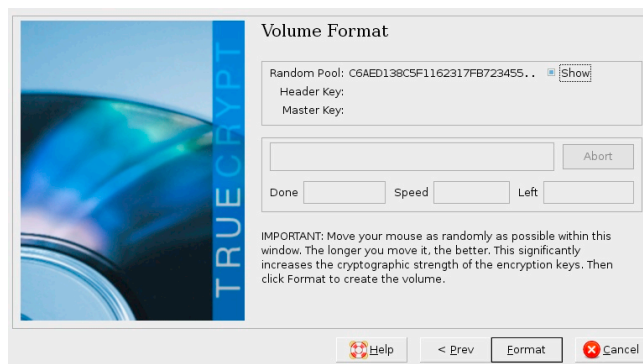


In questa finestra scegliete la password da utilizzare per l'accesso ai contenuti del contenitore cifrato. Leggete il testo che accompagna questa finestra per un suggerimento circa la scelta di una buona password. Una volta scelta, fate clic sul pulsante Next. La finestra di dialogo seguente vi chiede quale tipo di filesystem usare. L'unica opzione disponibile è FAT. Fate solo clic di nuovo sul pulsante Next (figura al centro in alto).

A questo punto, TrueCrypt ha tutte le

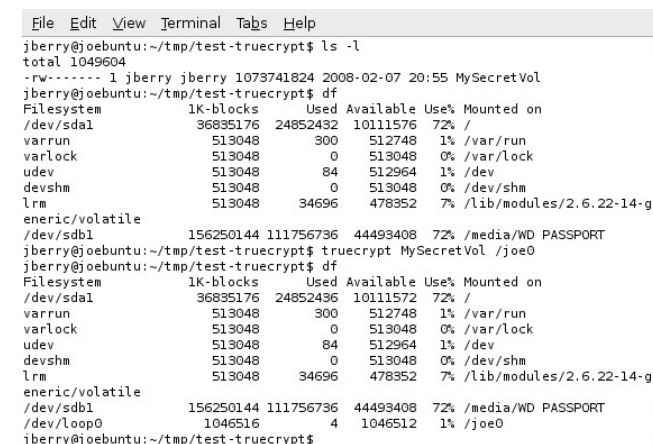


informazioni che gli servono per creare il volume. Di nuovo, leggete le istruzioni apparse nella nuova finestra di dialogo. In poche parole, dovrete muovere continuamente il mouse all'interno della finestra di dialogo per permettere la produzione di cifre casuali che TrueCrypt utilizza per creare il volume cifrato.

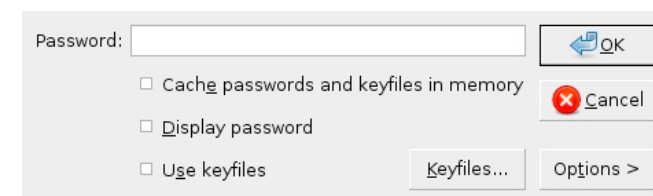


L'ultima finestra di dialogo è solo un indicatore di avanzamento che mostra la formattazione del volume con TrueCrypt. Una

volta completata, osservate il file creato e come possiamo "montare" il nostro nuovo filesystem col comando "truecrypt" nel terminale.



Quando si esegue il precedente comando "truecrypt" per montare il filesystem, appare una finestra che chiede l'immissione della password scelta prima. Notate che stiamo montando il volume nella directory /joe0. Per permettere ciò, prima bisogna creare la directory. Se non si specifica una directory, verrà utilizzata una directory predefinita.

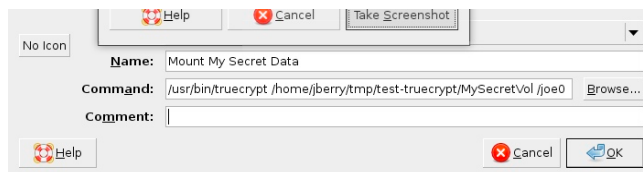


In alternativa, si può utilizzare la GUI (la prima finestra di dialogo che è apparsa quando avete immesso "truecrypt") per montare il file come un filesystem. Ho notato un comportamento anomalo con questa nuova versione di TrueCrypt. Una volta usciti dall'interfaccia grafica, si pensa che il programma TrueCrypt sia stato chiuso. Ma non è così. È necessario dare Ctrl-C nel terminale per terminare TrueCrypt.

Per smontare il filesystem (assicuratevi di non avere file aperti nel filesystem su cui avete appena lavorato) eseguite il seguente comando:

```
truecrypt -d /joe0
```

o qualunque sia la directory dove avete montato il contenitore di TrueCrypt. Diamo un tocco finale e automatizziamo il montaggio del filesystem di TrueCrypt. Sicuramente non vogliamo aprire una



finestra di terminale ed eseguire il comando truecrypt ogni volta che vogliamo accedere al nostro filesystem. Vogliamo soltanto fare doppio clic su un'icona. Su un'area vuota del vostro desktop GNOME fate clic destro col mouse e selezionate "Crea lanciatore...". Apparirà una finestra di dialogo (vedi la

figura a lato). In "Comando" immettete il seguente comando di TrueCrypt:

```
/usr/bin/truecrypt /home/joe/tmp/test-truecrypt/MySecretVol /joe0
```

Quando si fa clic su questa icona, apparirà una temporanea finestra di terminale, seguita da una finestra di dialogo che vi chiederà di immettere la password per questo contenitore. Immessa la password, la finestra si chiuderà. In modo simile, potete creare un lanciatore per smontare il filesystem. È tutto. Fate pratica creando un piccolo contenitore di TrueCrypt finché l'interfaccia vi risulterà comoda da usare, mentre saprete che i dati sono al sicuro, ma ancora accessibili. 🔒

In questo articolo mostrerò i passaggi che ho fatto per creare un account utente in Ubuntu per l'utilizzo da parte di mio nipote di sei anni. Anche se questa configurazione è specifica per le sue necessità, molte di queste considerazioni potrebbero essere valide per la configurazione di un account per un bambino.

Quando mio nipote ha cominciato a saperne di più e si è potuto fare affidamento sulla sua capacità di non fare danni intenzionali a qualcosa di delicato come un computer di casa, gli ho consentito un accesso controllato al mio computer. Lui lo usa soprattutto per divertirsi con dei giochi che ho installato per lui o per accedere ai siti delle sue reti TV preferite, come pbskids.org e sproutonline.com.

In ogni caso ha raggiunto un livello di capacità tale che raramente ha bisogno del mio aiuto. Mentre vorrei stare lì con lui e continuare a controllarlo direttamente, semplicemente non ne ho il tempo. Quindi in questo articolo, mostrerò i passaggi che ho fatto per creare un account utente in Ubuntu

per mio nipote di sei anni. Innanzitutto ho creato un account a parte per lui. In Gnome sono andato su Sistema > Amministrazione > Utenti e gruppi. Dopo aver immesso la mia password di amministratore si è aperta la finestra per le impostazioni Utenti. Ho cliccato su Aggiungi utente ed è apparsa la finestra Nuovo account utente.

Nella scheda account (qui sotto) ho immesso il nome utente che volevo assegnargli e il nome

reale. Ho scelto di impostare l'account come Non privilegiato e ho lasciato vuoti i campi con le informazioni sul contatto. Per la password, ne ho fatte generare molte finché non ne ho trovata una abbastanza complessa. Purtroppo le password generate casualmente non includono alcun carattere speciale ma può essere immesso direttamente in questo campo. Questa password era quasi impossibile da ricordare per mio nipote. Fortunatamente ciò non sarà un problema, lo spiegherò meglio fra poco.

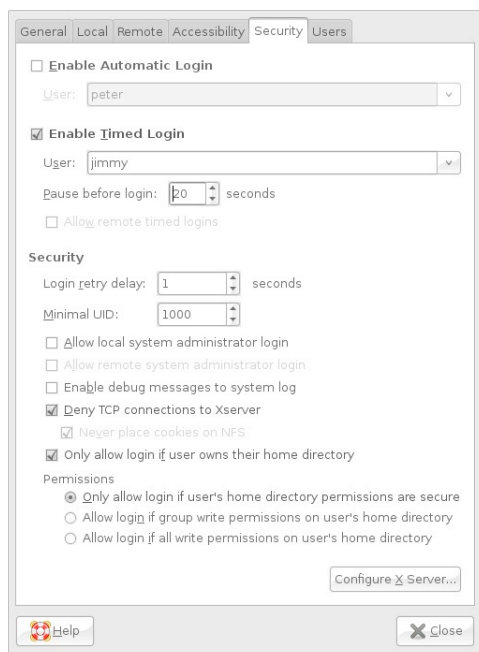
Poi ho cliccato sulla scheda Privilegi utente (accanto) e ho aggiunto i privilegi che volevo assegnare a mio nipote:

- Accesso automatico a dispositivi di memorizzazione esterni
- Utilizzo di dispositivi audio
- Utilizzo di unità CD-ROM.

Non c'era nulla che mi

interessasse nella scheda Avanzato, per cui ho cliccato OK e ho chiuso la finestra delle Impostazioni utenti.

Prima di uscire dal mio account sono andato in Sistema > Amministrazione > Finestra di accesso (a sinistra) per configurare il display manager di Gnome.



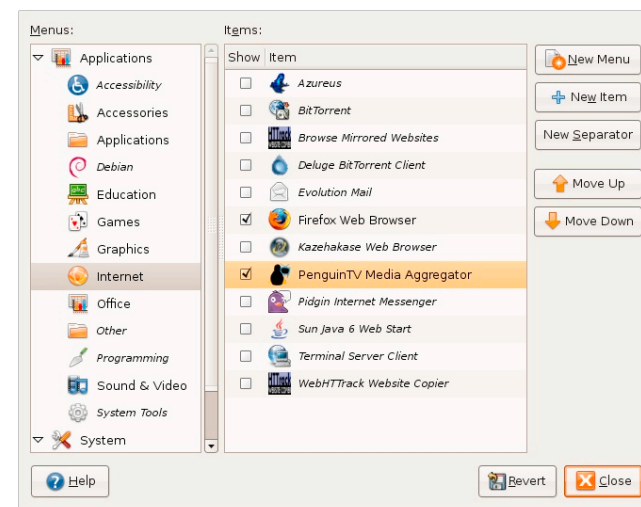
Nella finestra delle preferenze di accesso ho cliccato sulla scheda Sicurezza. Lì ho spuntato Abilitare accesso temporizzato, ho selezionato l'account di mio nipote nel menu a discesa e ho impostato la Pausa prima dell'accesso a 10

secondi. Ciò mi ha permesso di usare una password molto sicura, senza bisogno che mio nipote la memorizzasse. Fatto ciò, ho chiuso le preferenze di login e ho riavviato il mio computer prima di provare il login temporizzato.

Il mio obiettivo principale nel preparargli l'account era la semplicità d'uso per lui. Ho voluto semplificarlo il più possibile; potevo sempre complicarglielo in un secondo tempo. La prima cosa l'ho cambiata nelle Preferenze del selettore area di lavoro impostandogli il numero delle aree di lavoro a una. Poi ho rimosso del tutto questo selettore. Ho poi rimosso l'applet "Esci...".

Come regola generale, volevo evitare la confusione: volevo anzitutto che trovasse subito ciò che voleva usare, evitando nel frattempo che trovasse le cose che gli proibivo. Così la prossima cosa da ritoccare era il menu. Ho pensato di creare dei pulsanti sul desktop e di toglierli dal menu, ma ci sono troppi programmi per renderla una soluzione ottimale. Così, ho aperto Alacarte, l'editor di menu incluso in Ubuntu, e ho cominciato a selezionare.

Ci sono molti sotto-menu nell'installazione

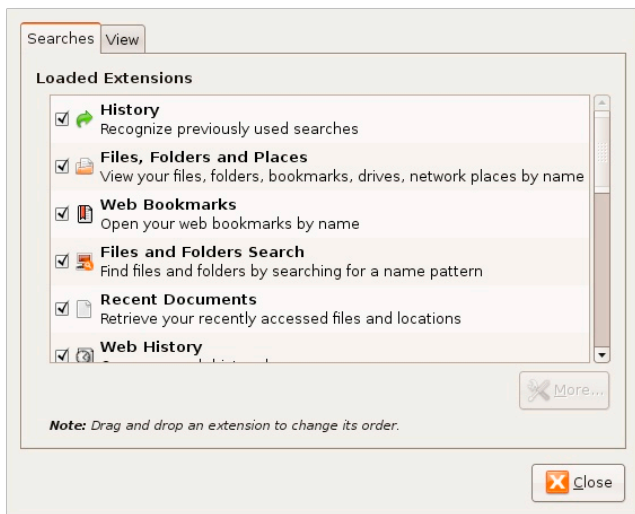


standard e poche preziose applicazioni che mi pare gli possano essere utili. Le mie scelte esposte qui furono specifiche per il mio caso; comunque essenzialmente ho rimosso la maggior parte delle preferenze, tutto il menu di amministrazione e tutte le voci dei programmi che non avevo installato specificamente per lui, fatta eccezione per elementi comuni come l'Editor di testo, la Calcolatrice e Firefox.

Anche se la voce di menu "Cerca file..." è disponibile nel menu Risorse, volevo rendere la ricerca più facilmente accessibile; così ho aggiunto Deskbar al pannello superiore e nella scheda Visualizzazione delle preferenze di Deskbar ho impostato la voce Aspetto come

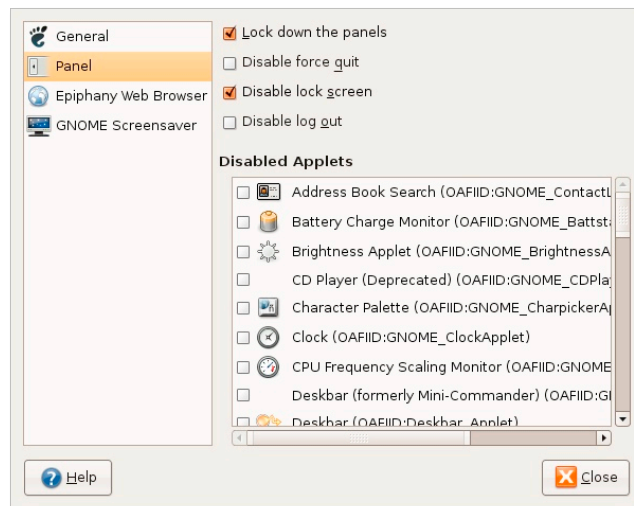
Casella di testo nel pannello. Ho poi disabilitato molte delle estensioni nella scheda Ricerche, lasciando solo:

- Cerca file e cartelle
- Cronologia
- Segnalibri web
- Cronologia web
- Documenti recenti



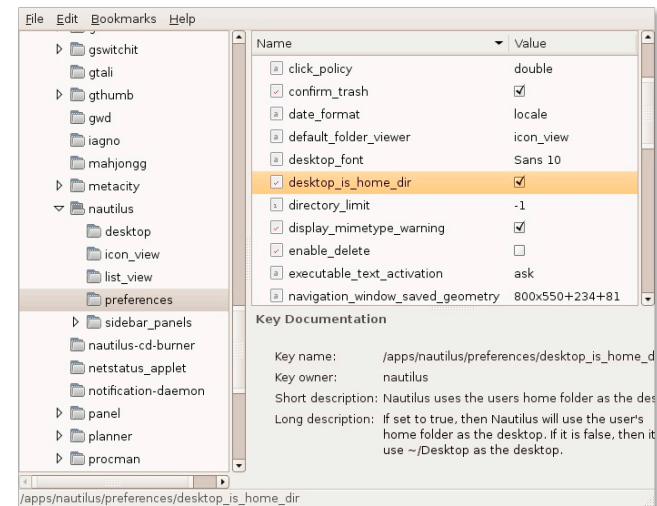
L'idea è sempre quella di limitare la quantità di informazioni che deve elaborare. Una volta configurati i pannelli a mio piacimento, ho avviato Pessulus, un editor per le impostazioni di blocco per Gnome. Non essendo installato in modo predefinito all'interno di Ubuntu, Pessulus è reperibile dai repository di Ubuntu. Non mi aspetto che

mio nipote provi effettivamente ad eludere le restrizioni che ho applicato per il suo account. Onestamente, se mi spingessi troppo lontano, non farei che incoraggiare che ciò accada. Così, a dispetto della molteplicità di opzioni di Pessulus, le mie necessità ora sono semplici. Spostandomi nella sezione "Pannello" di Pessulus, ho attivato due opzioni, "Blocca i



pannelli" e "Disabilita blocco dello schermo" (qui sopra), quindi ho chiuso l'editor di blocco. Si spera che ciò impedisca le tipiche "sparizioni" di pannelli e applet, la rovina dei nuovi utenti come anche delle assistenze tecniche. Come passo finale, ho eseguito gconf-editor e ho navigato fino ad apps > nautilus > preferences nel riquadro a

sinistra attivando desktop_is_home_dir (a destra). Questo modificherà la cartella della scrivania da /home/jimmy/Desktop a solamente /home/jimmy. Essendoci disparità di opinioni sul fatto che questa debba o meno essere un'impostazione predefinita in Gnome, credo che sia comunque appropriata vista la mia particolare situazione.



La prima parte di software che intendo configurare è Firefox. Ci sono molte valide risorse per gli studenti sul Web. Per non parlare della varietà infinita di giochi (una volta installati Flash e Java). Ad ogni modo possono essere trovate molte altre cose nelle selve di internet. Con questo in mente, perseguirò il mio giro usuale di

semplificazioni con una forte impronta di “controllo parentale”. In aggiunta a questo, ho installato un ad-blocker. Pur essendoci molti argomenti validi contro l'utilizzo delle fastidiose applicazioni pubblicitarie, mi sta molto più a cuore la protezione delle menti impressionabili dei bambini dal bombardamento del commercialismo.

Ora, come ho detto prima, uno dei miei obiettivi primari in tutto questo processo è stato semplificare le interfacce utente. A tal fine, la mia prima mossa con Firefox è stata rimuovere dalla barra di navigazione tutti i pulsanti tranne “Avanti” e “Indietro”, come

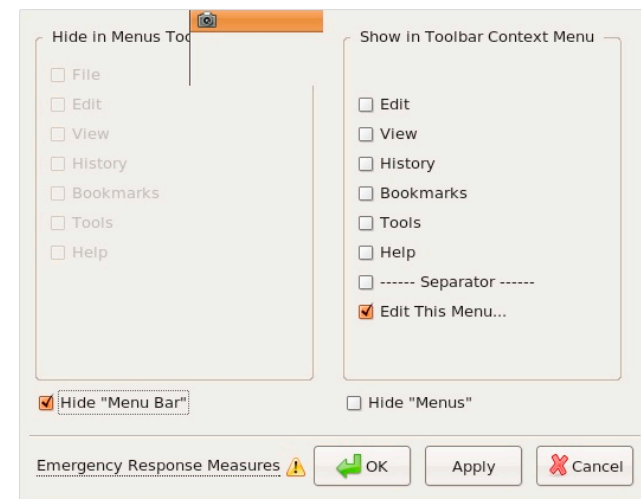
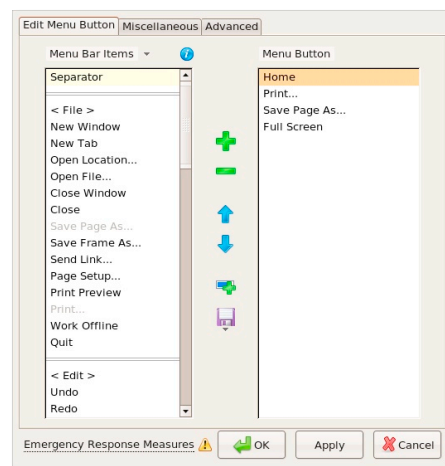


disabilitare l'utilizzo delle icone piccole nella finestra Modifica barre degli strumenti. Una volta soddisfatto del menu, ho cercato nella

pagina degli add-on di Mozilla una estensione chiamata Menu Personale e l'ho installata. La versione più recente al momento in cui scrivo questo documento è la 3.0.5. Una volta riavviato il mio browser, ho aperto le preferenze del Menu Personale. Menu Personale è un'estensione perfetta per semplificare l'interfaccia: permette di creare un pulsante per la barra degli strumenti di navigazione, spostare oggetti dai menu della barra standard (File, Modifica, Visualizza, ecc..) all'interno dei menu dei tuoi pulsanti, e quindi nascondere la barra dei menu. Così, dopo aver aggiunto le mie scelte dai menu standard, ho messo il menu personalizzato all'estrema destra della barra di navigazione, con la casella di ricerca proprio alla sua sinistra. Gli elementi che ho scelto sono più o meno standard:

- Home
- Stampa
- Salva pagina con nome...
- Schermo Intero

Ad eccezione di Salva



pagina con nome... nessuna di queste voci è disponibile nel menù contestuale predefinito.

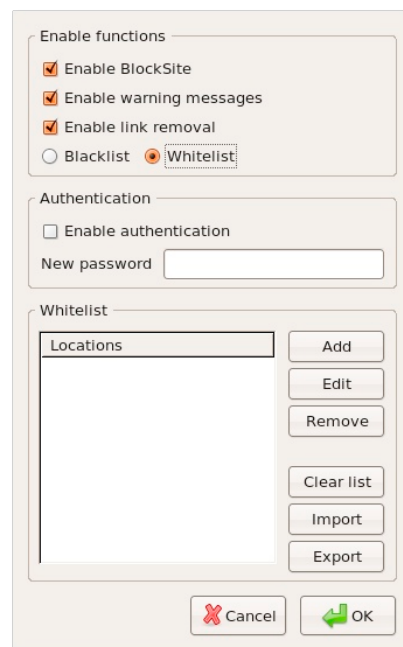
Come ho già detto in precedenza, non prevedo che mio nipote cerchi di superare

tutte le restrizioni che ho impostato al suo account. In questo modo semplifico il mio approccio nel limitargli l'accesso a Internet. Dopo essermi guardato un po' attorno ho trovato la soluzione che stavo cercando: un elenco degli indirizzi permessi.

La maggior parte delle soluzioni "controllo parentale" invece usa o una lista nera, un elenco di indirizzi vietati, o usa una combinazione di indirizzi vietati e di filtri sui contenuti che verificano la presenza di alcune parole-chiave all'interno della pagina richiesta. Ci sono numerosi svantaggi in questo tipo di approccio: alcune parole utilizzate in contesti non adatti possono avere anche un uso in un contesto normale; i creatori degli elenchi di indirizzi vietati non posso sperare di catalogare tutte le pagine esistenti, data l'enorme quantità di nuove pagine create ogni giorno; in cima a questi problemi concreti c'è il problema dei pregiudizi del responsabile sulle pagine che dovrebbero essere bloccate.

Per fortuna posso prendere questo tipo di decisioni da solo. Scegliendo una soluzione basata su un elenco di indirizzi permessi posso scegliere a quali pagine può accedere mio nipote. Qualunque pagina che non sia

nell'elenco delle pagine ammesse è automaticamente bloccata. Siccome l'interesse di mio nipote crescerà, dovrò verificare i soggetti a cui è interessato e permettere l'accesso a quelli che trovo accettabili. Sebbene ciò comporti un sforzo maggiore da parte mia, implica una miglior conoscenza tra noi.



l'uso o dell'elenco di indirizzi vietati o dell'elenco di indirizzi consentiti. I caratteri jolly sono supportati, in questo modo, aggiungendo `*wikipedia.org/*` è possibile

L'estensione che ho installato si chiama BlockSite (a lato) ed è disponibile alla pagina delle estensioni ufficiali di Mozilla Firefox. BlockSite ha un'interfaccia molto semplice e permette

accedere a tutte le pagine di ogni sotto dominio del sito wikipedia.org. Se ritenete di averne bisogno potete anche impostare una password che deve essere inserita per poter accedere alle preferenze di BlockSite. Ad ogni modo, l'intera estensione può essere disabilitata dalla finestra delle Estensioni, quindi non è una soluzione troppo efficace.

Per siti che vi danno problemi provate a verificare il proxy o il firewall. Per esempio, ho voluto aggiungere il sito `storylineonline.net`, che offre i filmati di attori professionisti mentre leggono libri per bambini. Il sito era caricato correttamente ma i video non erano riprodotti. Nella pagina di aiuto ho trovato il motivo. Il problema derivava dal fatto che i video si trovavano su un sito con un nome di dominio diverso. Aggiunto il dominio all'elenco degli indirizzi permessi, tutti i filmati venivano riprodotti correttamente.

Per quelli che desiderano una soluzione un po' più sicura esiste PublicFox, che sembra essere un'estensione di BlockSite con alcune modifiche che permettono che la password di protezione sia estesa ad altre funzioni come le preferenze del browser, la pagina `about:config` e la finestra delle estensioni. Io

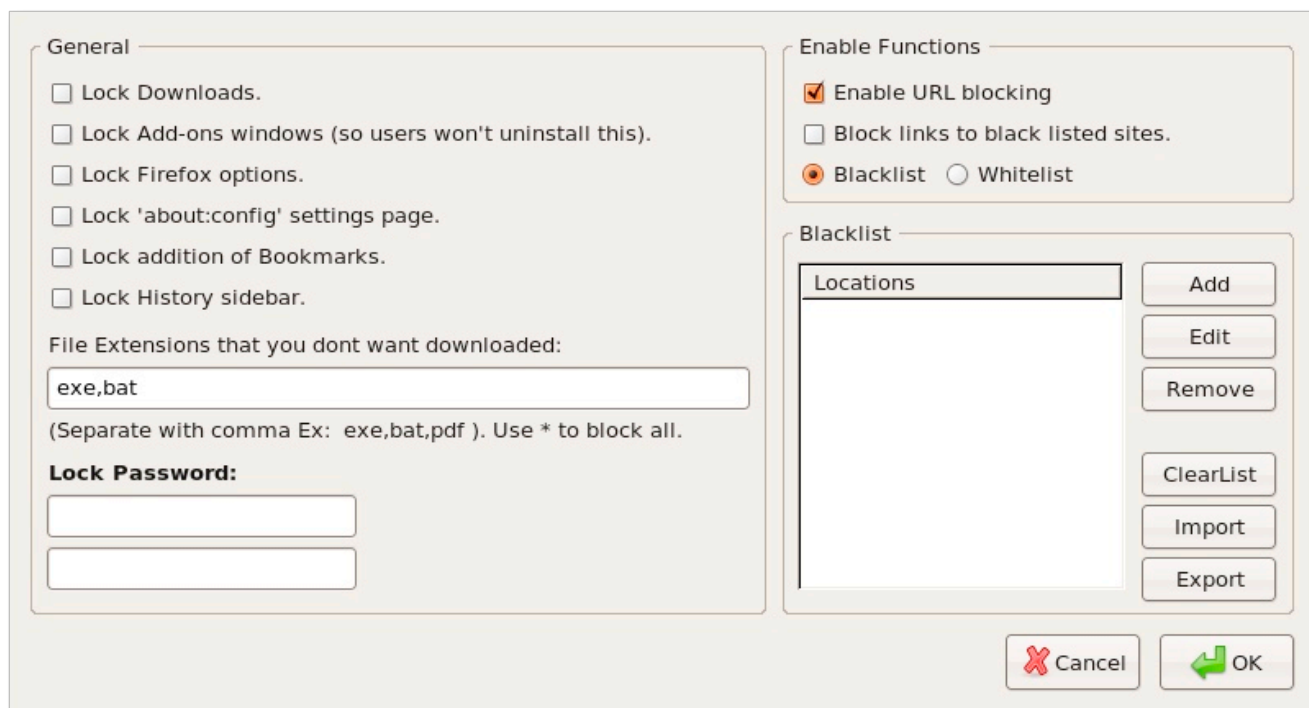
l'ho provato per un po', ma i continui pop-up per l'inserimento della password non rendono l'esperienza troppo amichevole. Utilizzato assieme con Pessulus per disabilitare la linea di comando e per prevenire l'esecuzione di Firefox attraverso il parametro `-profilemanager`, questa è una soluzione di blocco soddisfacente. Comunque c'è un modo per aggirare le restrizioni, presupponendo che sappiate come. In questo caso l'utente può semplicemente accedere alla cartella con il proprio profilo e modificare

alcuni file di testo per disabilitare l'estensione.

Questa è la mia configurazione. In futuro, se mio nipote inizierà a copiare le abitudini di download di suo zio, dovrò ricreare il suo account utilizzando le quote disco. Per chi fosse interessato a come impostare questa funzionalità, potrebbe essere di aiuto riferirsi al post di Aysiu nel forum di ubuntu qui: <http://ubuntuforums.org/showpost.php?p=2692744&postcount=10>. Se mai inizierà a

sviluppare insane abitudini informatiche, come ad esempio passare troppo tempo davanti al computer, lo stesso Gnome offre una soluzione. Sotto le impostazioni della tastiera, nelle preferenze di Gnome, c'è la linguetta "Pausa nella digitazione". La "Pausa nella digitazione" può essere impostata per bloccare lo schermo dopo un tempo predeterminato, regolabile da uno fino a centomila minuti con incrementi di un minuto. Se arriverò a tanto, dovrò impostare gdm per eseguire l'accesso automatico con l'account di mio nipote e memorizzarne la password. Sostanzialmente, direi che è un buon inizio.

Dato che il PC che utilizziamo è il mio, non ho trovato alcun motivo per installare edubuntu, ma ho comunque installato praticamente tutto il software educativo disponibile nel repository, oltre a uno che non c'è: Gutenpy. È un browser di cataloghi e un visualizzatore di testo del Progetto Gutenberg e lo consiglio caldamente. Anche se non c'è un rilascio specifico per Ubuntu, è disponibile un file .deb che ho utilizzato senza problemi, il pacchetto Debian è disponibile all'indirizzo <http://gutenpy.sf.net/> 





Editoria

Introduzione a LaTeX

Digitalizzare e convertire in PDF

Digitalizzare documenti in PDF/DJVU



LaTeX è un sistema di impaginazione che non segue il "normale" approccio WYSIWYG (What You See Is What You Get) degli elaboratori di testo a cui la maggior parte di noi è abituata. La forza di LaTeX sta nel fatto che segue delle regole di composizione molto simili a quelle sviluppate prima della comparsa degli elaboratori di testo. I documenti creati usando LaTeX sembreranno documenti impaginati in modo professionale. Uso LaTeX per creare lettere, documenti e presentazioni; l'ho persino usato per creare un grande poster a lavoro. Questo software è molto popolare nelle università grazie alla sua particolare capacità di manipolare equazioni e riferimenti incrociati. Questo articolo conterrà solo un piccolo assaggio di ciò che è possibile fare con questo sistema di impaginazione e tratterà quanto segue:

Pagina Titolo

Indice

Indice delle Figure

Indice delle Tabelle

Inserire un'immagine

Riferimenti Incrociati

Equazioni

Useremo il comando `pdflatex` per generare un PDF direttamente dal nostro "codice sorgente". Per prima cosa, installate LaTeX con il vostro gestore di pacchetti, installando ***texlive-latex-base***. Qui sotto c'è una lista di comandi utilizzati per creare il contenuto del documento. Inserite il seguente codice in marrone in un file di testo

```
.\documentclass[a4paper,12pt]{article}
\usepackage{graphicx}
\usepackage{multicol}
```

```
\title{LaTeX Primer}
\author{TUX}
```

```
\begin{document}
\maketitle
\clearpage
\tableofcontents
\clearpage
\listoftables
\clearpage
\listoffigures
\clearpage\section{Equations}
```

Inizierò aggiungendo nel documento una famosa equazione e facendo riferimento

ad essa nel testo. Nel 1905 Einstein pubblicò degli articoli importanti, uno di questi era Relatività Speciale, nota ai più come `\ref{eq-n1}`.

```
\begin{equation}
\label{eqn1} E = mc^2
\end{equation}
```

dove E è l'energia, m la massa dell'oggetto e c la velocità della luce.

```
\section{Table}
```

Adesso inseriremo una tabella contenente una lista di nomi ed età di fantasia. La Tabella `\ref{table1}` contiene...

```
\begin{table} [!h]
\caption{Una tabella contenente età e nomi}
\label{table1}
\begin{center}
\begin{tabular}{|c|c|}
\hline
Nome & Età \\
\hline
\end{tabular}
\end{center}
\end{table}
```

```
\hline
Bob & 24\\
Dave & 13\\
Lucy & 27\\
Claire&12\\
\hline
\end{tabular}
\end{center}
\end{table}
```

```
\section{Columns}È molto facile
aggiungere colonne multiple al docu-
mento:
```

```
\begin{multicols}{2}
TESTO TESTO TESTO TESTO TESTO TESTO
TESTO TESTO TESTO TESTO TESTO TESTO
TESTO TESTO TESTO TESTO TESTO TESTO
TESTO TESTO TESTO TESTO TESTO TESTO
\end{multicols}
```

```
\section{Image}
\begin{figure}[!h]
\caption{Image}
\label{image1}
\begin{center}
\includegraphics[width=3in]{tux.png}
\end{center}
```

```
\end{figure}
\end{document}
```



L'immagine "tux.png" usata nel codice.

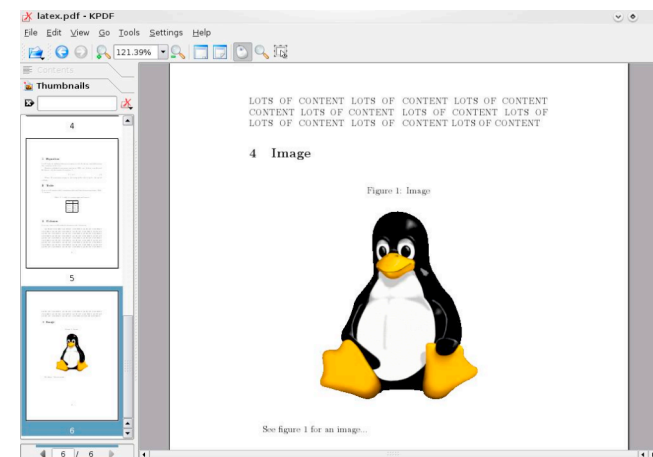
Una volta completato salvate il file in un posto conosciuto, aprite un terminale e posizionatevi nella cartella dove lo avete salvato. A questo punto digitate:

```
pdflatex fullcircle.tex
```

Per generare dei riferimenti incrociati il comando precedente va dato due volte.

Con questo tutorial ho fatto un'analisi a malapena superficiale e raccomando di leggere *The Not So Short Introduction to LaTeX 2E* ("Una mica tanto breve introduzione a LaTeX 2e")

<http://www.ctan.org/tex-archive/info/lshort/english/lshort.pdf> 

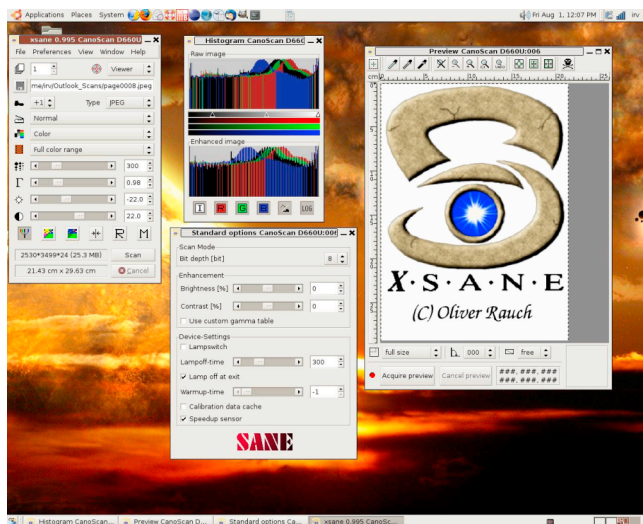


Il PDF finale così come appare in KPDF.

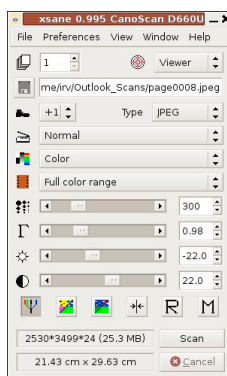
Il mio problema era riuscire a mettere su Internet una vecchia newsletter in formato PDF, ma l'unica cosa che avevo era una copia cartacea. Ho provato a farlo su una macchina con installato Windows, ma dopo qualche tentativo ho desistito e ho avviato il mio portatile con Linux.

La prima cosa che dovevo fare era collegare il mio scanner con il portatile. Nessun problema, ha riconosciuto la periferica perfettamente.

A questo punto mi piacerebbe potervi dire che potete effettuare le scansioni direttamente da OpenOffice Writer, ma ho avuto problemi con il loro “Seleziona la sorgente di scansione”. Tutto è in millimetri anziché pollici e le uniche opzioni per il DPI sono 50 o 1200, per cui agiamo in maniera leggermente differente. Avrete bisogno dell'applicazione “Xsane”, presente nei Repository. Se non lo avete installato, fatelo come prima cosa. Andate nel pannello dei menu e selezionate Applicazioni > Grafica > Xsane – Scanner di immagini. L'ho impostato in modo da fargli aprire quattro finestre (nella figura in basso).



1. Finestra principale Xsane (sinistra)
2. Finestra degli istogrammi (in alto al centro)
3. Finestra delle opzioni (in basso)
4. Finestra dell'anteprima (destra)



Nella finestra principale ho impostato il percorso, il tipo di file (JPEG) e la risoluzione (300). Ho lasciato tutte le altre impostazioni quelle predefinite.



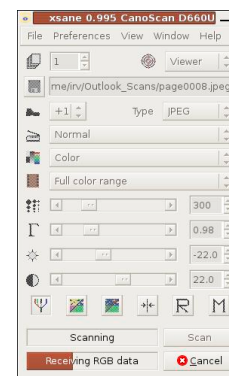
Nella finestra dell'anteprima, ho impostato la scansione a tutta pagina e lanciato l'acquisizione dell'anteprima.

Dopo aver ottenuto l'anteprima (facendo clic su “Acquisisci

anteprima”), selezionate l'area da scannerizzare spostando i righelli nella finestra dell'anteprima (osservate la linea

tratteggiata attorno all'immagine scansionata nella figura in alto), quindi andate nella finestra principale e fate clic sul pulsante Scansione.

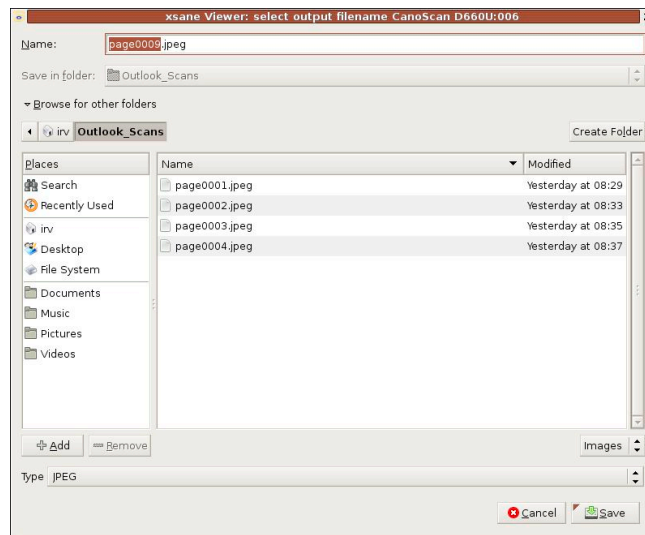
Quando la scansione è stata ottenuta, si aprirà la





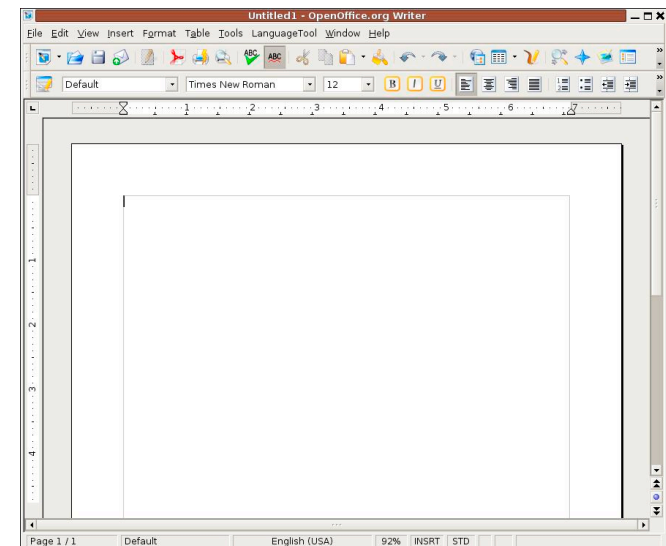
finestra del visualizzatore di immagini che illustra il risultato finale.

Adesso bisogna salvare la scansione andando nel menu File > Salva immagine.



Se usate il nome file impostato come predefinito, salverà le scansioni come pagina0001, pagina0002, ecc. Nel mio caso, avevo bisogno di realizzare 4 scansioni. Non appena ho finito, mi è bastato chiudere il visualizzatore di immagini e la finestra principale, che le altre finestre sono sparite automaticamente.

Adesso vediamo come fare per convertirle in un bel documento in formato PDF. Aprite OpenOffice.org Writer dal vostro menu Applicazioni. Si aprirà con un documento vuoto (destra). Con il puntatore andate al di sopra della prima pagina e selezionate il menu: Inserisci > Immagine > Da file...



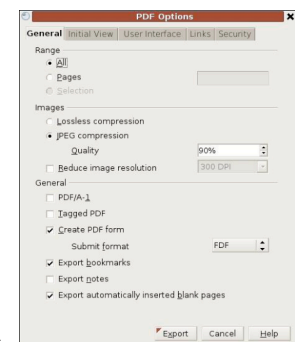
Selezionate il file che volete inserire e cliccate su Apri.

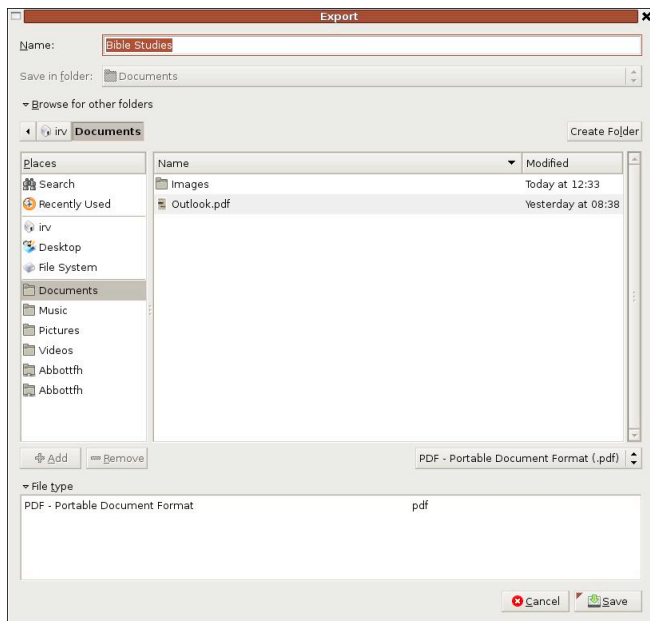
Posizionando poi il cursore all'inizio della pagina seguente, ripetete l'operazione finché non avrete tutte le scansioni effettuate nel vostro documento OpenOffice. Dopo di ciò, vogliamo esportare il tutto in formato PDF.

Possiamo farlo andando nel menu: File > Esporta nel formato PDF.

Non appena si apre la nuova finestra, lasciate tutto impostato come predefinito e selezionate il pulsante "Esporta".

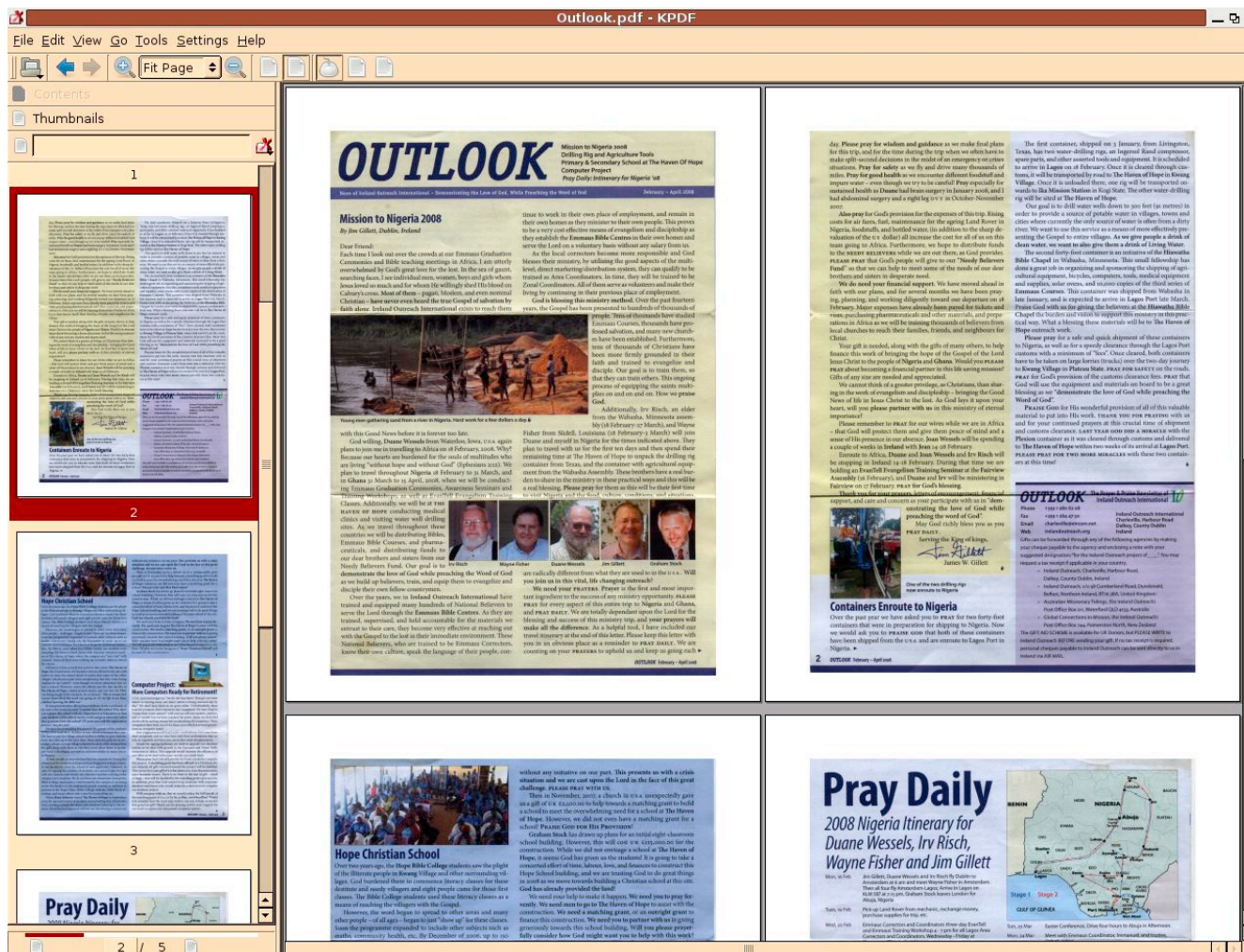
Si aprirà la finestra per il





salvataggio del documento, dove potete scegliere dove salvare il documento realizzato. Verrà salvato come documento formattato in PDF. Dopo aver chiuso il vostro documento in OpenOffice Writer, potete lanciare un'anteprima del lavoro finito. Andate dove avete salvato il vostro file e apritelo con il vostro visualizzatore di documenti in PDF.

Ecco come il mio documento finito viene visualizzato con KPDF.



Per terminare il mio lavoro, ho aperto Firefox, selezionato il plugin FireFTP e ho caricato il file sul mio server Web. Se volete

vederlo, lo potete trovare all'indirizzo <http://wabasha-server.net/Outlook.pdf>

Conservate le vostre riviste e i vostri documenti facendone una scansione e convertendoli nel formato PDF/DjVu prima che ingialliscano, vengano ridotti in pezzi e si perdano per sempre.

Col vostro scanner collegato siete pronti per l'operazione. Innanzitutto installate **gscan2pdf**. Il suo sito è <http://gscan2pdf.sourceforge.net> È anche nei repository. Per installarlo dal terminale, digitate:

```
sudo apt-get install gscan2pdf
```

Già che ci siete, installate **pdftk**. È il coltellino svizzero che uso per manipolare tutti i miei file PDF.

```
sudo apt-get install pdftk
```

Avrete anche bisogno di **pdf2djvu** cosicché, una volta ottenuti i vostri PDF in alta qualità, potete convertirli nel formato djvu a 400 dpi e risparmiare tanto spazio ma conservando i dettagli dei documenti. Quindi, di nuovo, digitate nella shell:

```
sudo apt-get install pdf2djvu
```

Questo è tutto quello che vi serve. Iniziamo la scansione!



Avviate **gscan2pdf** a fate clic sul pulsante di scansione. Con un po' di fortuna il vostro scanner USB verrà automaticamente selezionato, lo vedrete e potrete cambiarne alcuni parametri. Lo scanner che sto usando è un HP Scan-jet 6300 con un ADF (il dispositivo di alimentazione automatica degli originali) da 25 fogli. Per coloro

che non sanno cosa sia un ADF, assomiglia un po' a un fax. Posso anche scegliere la velocità di acquisizione. Io scelgo sempre la più veloce. Quindi, scegliete la risoluzione: io scelgo sempre 300 dpi. Ora, selezionate la modalità di scansione:

Tratto
Mezzitoni
Grigio
Colore

Tratto è in pratica una scansione in bianco e nero con una differenza molto piccola nel colore del nero/grigio. È perfetta per le pagine che sono soltanto in nero. **Non usate questa modalità se ci sono foto nella pagina.** Appaiono orribili. Questa modalità richiede poco spazio.

Mezzitoni acquisisce un originale con toni di nero molto intensi e lo rende con un aspetto davvero cupo sul vostro PC. Non uso mai questa modalità.

Scala di grigio. Usate questa modalità se avete una rivista in bianco/nero con foto. Questa modalità vi darà una riproduzione

davvero buona in bianco e nero. Occupa un po' di spazio ma non quanto quella a colori.

Colore. Questa si spiega da sé.

Per ottenere una rivista scansionate 10 o 20 pagine e salvate il lavoro nel formato PDF. Ci sono diverse opzioni per salvare le pagine digitalizzate. Potete salvare le pagine singole o salvare tutte le pagine come un unico PDF. Potete anche scegliere se usare il jpeg così come altri formati.

Dalle mie prove ho imparato ad usare la compressione jpeg quando salvo i PDF. Il jpeg è un "formato con perdita", per cui per non perdere in qualità salvo con un valore di qualità dell'84%. Se salvo all'85%, le dimensioni del file crescono a proporzioni

incredibili. Ripetete questa procedura di scansione per il vostro libro e concluderete con i vostri dati salvati in una directory con nomi di file del tipo:

```
mia.rivista.parte1.pdf
mia.rivista.parte2.pdf
mia.rivista.parte3.pdf
mia.rivista.parte4.pdf
mia.rivista.parte5.pdf
```

A mo' di esempio, immaginate che ogni file contenga 20 pagine e pesi 20 mega. Una volta uniti insieme, avrete un singolo PDF di 100 mega con le pagine in ordine numerico.

Per ottenere ciò, tornate di nuovo alla shell, puntate verso la directory dove avete salvato i file e avviate pdftk. Esso vi permetterà ogni sorta di intervento sui file PDF. In questo caso lo userete per unire i singoli file PDF in un unico grande file. Il programma lo farà senza battere ciglio. Ha tante funzioni, ma non le analizzerò qui. Nella shell digitate:

```
pdftk mia.ri
```

Ora premete il tasto Tab e magicamente vedrete apparire:

```
pdftk mia.rivista.parte
```

Ve lo avevo detto che la shell è potente. Ha scansionato la directory e magicamente ha aggiunto per voi "vista.parte". Ora premete 1 in modo da avere:

```
pdftk mia.rivista.parte1
```

Premete di nuovo Tab e vedrete:

```
pdftk mia.rivista.parte1.pdf
```

Intelligente, vero? Ripetete ora il procedimento di premere Tab e digitare 2, 3, 4 e 5 quando necessario e in pochi secondi avrete questo comando

```
pdftk mia.rivista.parte1.pdf
mia.rivista.parte2.pdf
mia.rivista.parte3.pdf
mia.rivista.parte4.pdf
mia.rivista.parte5.pdf
```

Ora dovrete dire a pdftk che volete unire questi file insieme in un unico grande file. Quindi aggiungete:

```
cat output mia.rivista.pdf verbose
```

Aggiungetelo alla fine di quello che avete digitato poco fa. Quindi l'intero comando apparirà così:

```
pdftk mia.rivista.parte1.pdf
mia.rivista.parte2.pdf
mia.rivista.parte3.pdf
mia.rivista.parte4.pdf
mia.rivista.parte5.pdf cat output
mia.rivista.pdf verbose
```

Il comando `verbose` alla fine dice alla shell di far vedere sullo schermo quello che fa il programma. Vi risparmierà di indovinare quello che sta succedendo. Se non fate così, non avrete alcuna risposta dal programma, una volta che avrete premuto Invio. Premete quindi Invio e osservate scorrere le pagine. In pochi secondi tornerete al prompt dei comandi col cursore lampeggiante.

Guardate ora nella directory e vedrete il documento finale col nome `mia.rivista.pdf`. Apritelo (col vostro visualizzatore di documenti/PDF) e scorretelo per ammirare il documento da 100 pagine che avete messo assieme. Osservate ora le dimensioni del file. Immagino che sarà di circa 110 mega o forse meno.

Per convertirlo nel formato djvu e mantenere le pagine in alta qualità ma con un file di minori dimensioni, aprite la shell e digitate:

```
pdf2djvu -o mia.rivista.djvu -d400 -v
mia.rivista.pdf
```

Per spiegarlo un po', avete detto al programma che il file finale sarà chiamato `mia.rivista.djvu`, che volete comprimerlo usando 400 dpi (con `-d400`), che volete vedere l'output a schermo per sapere cosa sta succedendo (con `-v`) e che il nome del file di partenza è `mia.rivista.pdf`. Ora premete Invio. Vedrete qualcosa di simile:

```
mia.rivista.pdf:
- page #1 -> #1:
- image size: 3199x4332
- 353010 bytes out
- page #2 -> #2:
- image size: 3199x4332
(NOTA DELL'AUTORE: ho cancellato molte
  pagine da questa sezione)
- 341857 bytes out
- page #76 -> #76:
- image size: 3167x4332
- 450144 bytes out
0.210 bits/pixel; 3.858:1,
74.08% saved, 105702515
```

bytes in, 27394816 bytes out

Avete capito come funziona.

Ora guardate nella directory a vedrete il vostro file `.djvu`, i vostri singoli PDF di partenza e il PDF finale. Cancellate tutti i file `.parte1.pdf` ma conservate il PDF finale e i file DjVu. Potete fare ciò andando nella directory dove stavate lavorando, selezionando i file e premendo il tasto Canc. Non cancellate il grande file PDF. I file PDF sono più semplici da lavorare rispetto a quelli DjVu. Fate quindi le modifiche ai grandi file PDF e poi rigenerate il file DjVu.

Quando digitalizzate le pagine, assicuratevi di correggere i valori di luminosità/contrasto sul software **gscan2pdf**. Potreste aver bisogno di aumentare il contrasto/luminosità a 30 o a 40 quando scansionate a colori per ridurre la trasparenza delle pagine e dare uno sfondo netto. Ho constatato che bisogna farlo quando si usa la modalità Tratto. Ciò aiuta anche a ridurre l'ingiallimento dei fogli delle vecchie riviste e a ridurre le dimensioni del file. Fate delle prove con queste impostazioni. Impiegate un po' di tempo armeggiando un po' prima di impazzire e scansionare alcune centinaia di libri. ❌

DAL 2007 A OGGI HANNO COLLABORATO ALLA REALIZZAZIONE DELLA RIVISTA

*Antonino Arcudi
Vito Luca Arnetta
Michele Azzolari
Giuseppe Calà
Milo Casagrande
Dario Cavedon
Teo Cocetta
Luca De Julis
Roald De Tino
Luigi Di Gaetano
Gerardo Di Giacomo*

*Edoardo Elidoro
Cristina Franzolini
Paolo Garbin
Fabrizio Giacosa
Mattia Impellizzeri
Aldo Latino
Marco Letizia
Cristiano Luinetti
Luca Manganelli
Maurizio Moriconi
Paolo Naldini*

*Davide Notaristefano
Istituto Pacinotti
Lidia Pellizzaro
Antonio Piccinno
Luca Saba
Valerio Salvucci
Mara Sorella
Gianfranco Taormina
Vito Tigani
Flavia Weisghizzi*



A cura della Comunità di Ubuntu Italia - Progetto FCM